EUROPEAN
COMMISSION

Brussels, 17.4.2018
SWD(2018) 118 final

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT**

***Accompanying the document***

**Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters**
**and**
**Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings**

{COM(2018) 225 final} - {COM(2018) 226 final} - {SWD(2018) 119 final}

## Table of Contents

## Glossary

| *Term/Acronym* | *Definition* |
|---|---|
| Access logs | Access logs record the time and date an individual has accessed a service and the IP address from which the service was accessed |
| Budapest Convention | 2001 Council of Europe Convention on Cybercrime |
| Cloud computing | Model for enabling convenient on-demand network access to a shared pool of configurable computing resources |
| Connecting factor | A fact that connects an occurrence with a particular law or jurisdiction |
| Content data | The substance of stored information, such as text, voice, videos, images, and sound |
| Data sharding | A type of database partitioning that is used to separate very large databases the into smaller, faster, more easily managed pieces called data shards |
| e-CODEX | IT system for cross border judicial cooperation which allows users to send and receive documents, legal forms, evidence etc. in a secure manner |
| ECPA | 1986 US Electronic Communications Privacy Act of 1986 |
| E-evidence | Electronic evidence:, electronically stored data such as subscriber information, metadata or content data, generated by any activity related to digital services |
| EIO | European Investigation Order, as set out in Directive 2014/41/EU |
| ETSI | European Telecommunications Standards Institute |
| International Comity | The practice of showing courtesy among nations, the disposition to perform some official act out of goodwill and tradition rather than obligation or law |
| IP address | Internet Protocol address, a unique identifier allowing a device to send and receive packets of information; a basis for connecting to the internet |
| Judicial authority | A judge, a court, an investigating judge or a public prosecutor |
| Loss of location | A situation where law enforcement cannot establish the physical location of the perpetrator, the criminal infrastructure or electronic evidence. |
| Metadata | Data processed for the purposes of transmitting, distributing or exchanging electronic communications or other content through a network |
| MLA(T) | Mutual Legal Assistance (Treaty) |
| Production order | An order issued by the competent authority of a Member State to a digital service provider to provide specified electronic evidence |
| Production request | A request without a binding effect by the competent authority of a Member State to a digital service provider to provide specified electronic evidence |

| *Term/Acronym* | *Definition* |
|---|---|
| Ransomware | A type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid |
| SIRIUS | Europol platform to facilitate online investigations, including the direct cooperation between authorities and service providers |
| Subscriber information | Information allowing to identify a natural person or legal entity using services provided by relevant service providers |
| TOR | 'The Onion Router', an open source software that enables anonymous communication |
| Traffic data | Data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof |
| Transaction logs | Transaction logs identify products or services an individual has obtained from a provider or a third party (e.g. purchase of cloud storage space) |
| VPN | Virtual private network: a technology that creates a safe and encrypted connection over a less secure network, such as the internet |
| WHOIS | Reference database for ownership of web site domain names |

# 1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

## 1.1. Introduction

Cross-border data flows are rising together with the growing use of social media, webmail, messaging services and apps to communicate, work, socialise and obtain information, including by criminals. An increasing number of criminal investigations therefore rely on electronic evidence that is not publicly available, e.g. information on the holder of an email account, messages exchanged via Facebook messenger or information on the timing of WhatsApp calls.

Law enforcement and judicial authorities often experience difficulties in accessing electronic evidence relevant to an investigation. Electronic evidence is increasingly available only on private infrastructures, which may be located outside the investigating country, owned by service providers established outside the investigating country, or both. For such cross-border situations, traditional mechanisms for cooperation between authorities are slow compared to the fast pace at which data can be moved, changed or deleted. In addition, they are under increasing strain with the growing number of cross-border cases. Furthermore, authorities have begun to question whether a mechanism designed to protect the sovereignty of another country is apt for today's situations where the connection of the crime to the requested country is often limited.

In addition, information that is publicly available and easily accessible to law enforcement might move into systems requiring special credentials to access. This development notably concerns the general world-wide lookup tool for owners of web site domain names, known as "WHOIS"[1].

Direct cooperation with US service providers has developed as an alternative channel to judicial cooperation, but is limited to non-content data and is voluntary from the perspective of US law. In the face of these developments, a number of countries have begun to explore under what conditions authorities may request access to data using their own domestic tools. The Yahoo![2] and Skype[3] decisions in Belgium are examples of recent court cases which focus on the legitimacy of the use of domestic production orders for companies whose main seat is outside the requesting country but which provide a service in the territory of that country. The resulting fragmentation may generate legal uncertainty, as well as concerns on the protection of fundamental rights and procedural safeguards for the persons related to such requests.

---

1 Please see Annex 12 for further information.

2 Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N of 1 December 2015.

3 Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12 of 27 October 2016. It has been reported that Skype has appealed the decision.

In addition, there have been a number of court cases in the US on whether US authorities have the right to request the production of data stored abroad by a service provider whose main seat is in the US, including notably the "Microsoft Ireland" case[4].

Improving cross-border access to e-evidence is a pressing issue concerning almost any type of crime. In particular, the recent terrorist attacks have underlined the need, as a matter of priority, to find ways to secure and obtain e-evidence more quickly and effectively.

### 1.2. Political and legal context

The Commission committed in the April 2015 European Agenda of Security[5] to review obstacles to criminal investigations into cyber-enabled crimes, notably on cross-border access to electronic evidence. In April 2016[6] the Commission undertook to propose solutions by summer 2017, including legislation if required.

There have been repeated calls for action both from the EU Member States and the European Parliament. The Council supported the Commission´s commitment in its June 2016 Conclusions on improving criminal justice in cyberspace[7] and endorsed a set of practical measures to be taken forward. Specifically, the Council called on the Commission to take concrete actions based on a common EU approach to make mutual legal assistance more efficient, to improve cooperation between Member States' authorities and service providers based in non-EU countries, and to propose solutions to the problems of determining and enforcing jurisdiction[8] in cyberspace. The Review Report of the 2016 EU-US MLA Agreement, which was finalised at the same time as the Council Conclusions, contained several recommendations to improve access to electronic evidence[9]. In its final report on the seventh round of mutual evaluations on prevention and combating cybercrime[10], the Council also recommended that the EU and its Member States consider the development of an EU framework on law enforcement access to data held by service providers.

---

4 U.S. Court of Appeals for the Second Circuit, Microsoft v. United States, No. 14-2985 (2d Cir. 2016) of 14 July 2016. The case is under review by the U.S. Supreme Court and a decision is expected by July 2018. See http://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/ and Box 1 in Annex 9 on Microsoft case for more details.

5 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security, COM(2015) 185 final.

6 Communication on delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, COM/2016/0230 final.

7 Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST9579/16.

8 In this document, the term "enforcement jurisdiction" makes reference to the competence of the relevant authorities to undertake an investigative measure.

9 See Annex 5.

10 Council of the EU, Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime", ST 12711 2017 INIT, 2 October 2017.

President Juncker committed to put forward a legislative proposal in 2018 in his September 2017 Letter of Intent[11]. The European Parliament adopted a resolution on the fight against cybercrime in October 2017[12], which acknowledges the difficulties of public authorities in accessing electronic evidence across borders and underlines the need for a common European approach to criminal justice in cyberspace, as a matter of priority. It calls on the Commission to put forward a European legal framework for electronic evidence, including harmonised rules to determine the status of a provider (domestic or foreign), and to impose an obligation on service providers to respond to requests from Member States that are based on due legal process.

The legal and policy environment surrounding this initiative is complex because:
1) The initiative touches upon several areas:

- while cross-border access to evidence by public authorities in the framework of criminal investigations is governed by the acquis in the area of judicial cooperation in criminal matters, the initiative also involves exchange of personal data, so the data protection and ePrivacy frameworks are also relevant;
- there are many co-existing levels of regulation: EU law, rules at Member State level governing criminal investigations, international conventions and bilateral agreements. US law also plays an important role, as major service providers holding relevant evidence operate under US jurisdiction.

2) Some aspects of the legal environment are currently subject to changes:

- several EU instruments are currently under revision, such as the ePrivacy Directive, and new proposals are being prepared;
- work has recently started on an additional protocol to the Council of Europe Budapest Convention on Cybercrime, the main international framework governing access to electronic evidence by public authorities;
- like the EU and its Member States, the US is trying to address the issues created by cross-border access to e-evidence through legislative initiatives.

A detailed list of relevant legislation and policy can be found in Annex 5.

## 2. PROBLEM DEFINITION

Table 1 shows the intervention logic (problem, drivers, objectives and options) that will be described in detail in the following sections 2 to 5:

[11] State of the Union 2017, Letter from Commission President Juncker to President Antonio Tajani and to Prime Minister Jüri Ratas, 13 September 2017.

[12] European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)).

*Table 1: problem, drivers, objectives and options (intervention logic)*

| **Problem** | **Problem drivers** | **General objective** | **Specific objectives** | **Options** | | | |
|---|---|---|---|---|---|---|---|
| | | | | **Non-legislative** | **Legislative** | | |
| | | | | **A** | **B** | **C** | **D** |
| Some crimes cannot be effectively investigated and prosecuted in the EU because of **challenges** in **cross-border access to electronic evidence** | 1. It takes **too long** to access e-evidence across borders under existing judicial **cooperation** procedures, rendering investigations and prosecutions less effective<br>2. Inefficiencies in **public-private cooperation** between service providers and public authorities hamper effective investigations and prosecutions<br>3. Shortcomings in defining **jurisdiction** can hinder effective cross-border investigations and prosecutions | Ensure effective investigation and prosecution of crimes in the EU by **improving cross-border access to electronic evidence** through **enhanced judicial cooperation** in criminal matters and an **approximation** of rules and procedures | 1. **Reduce delays** in cross-border access to electronic evidence<br>2. **Ensure** cross-border **access** to electronic evidence where it is **currently missing**<br>**3.** Improve **legal certainty, protection of fundamental rights, transparency and accountability** | P**ractical measures** to enhance **judicial cooperation** between public authorities and **direct cooperation** between public authorities and service providers | Option A + **international** agreements | Option B + direct cooperation legislation on the **European Production Order** and access to **databases** | Option C + **direct access** legislation |

## 2.1. What is the problem?

### 2.1.1. Definition and magnitude

The problem is that some crimes cannot be effectively investigated and prosecuted in the EU because of **challenges** in **cross-border access to electronic evidence.**

Electronic evidence – which can be relevant for any crime – is often stored outside the country whose authorities need access. Determining the location of the data may be difficult, and even where it is possible, data can be moved quickly and effortlessly[13]. Once a cross-border element is or might be present, authorities have to rely on one of the three channels existing today to access e-evidence across borders:

1. judicial cooperation between public authorities,
2. direct cooperation between a public authority and a service provider and
3. direct access to electronic evidence by a public authority.

These channels suffer from a number of shortcomings that can be summarised as follows:

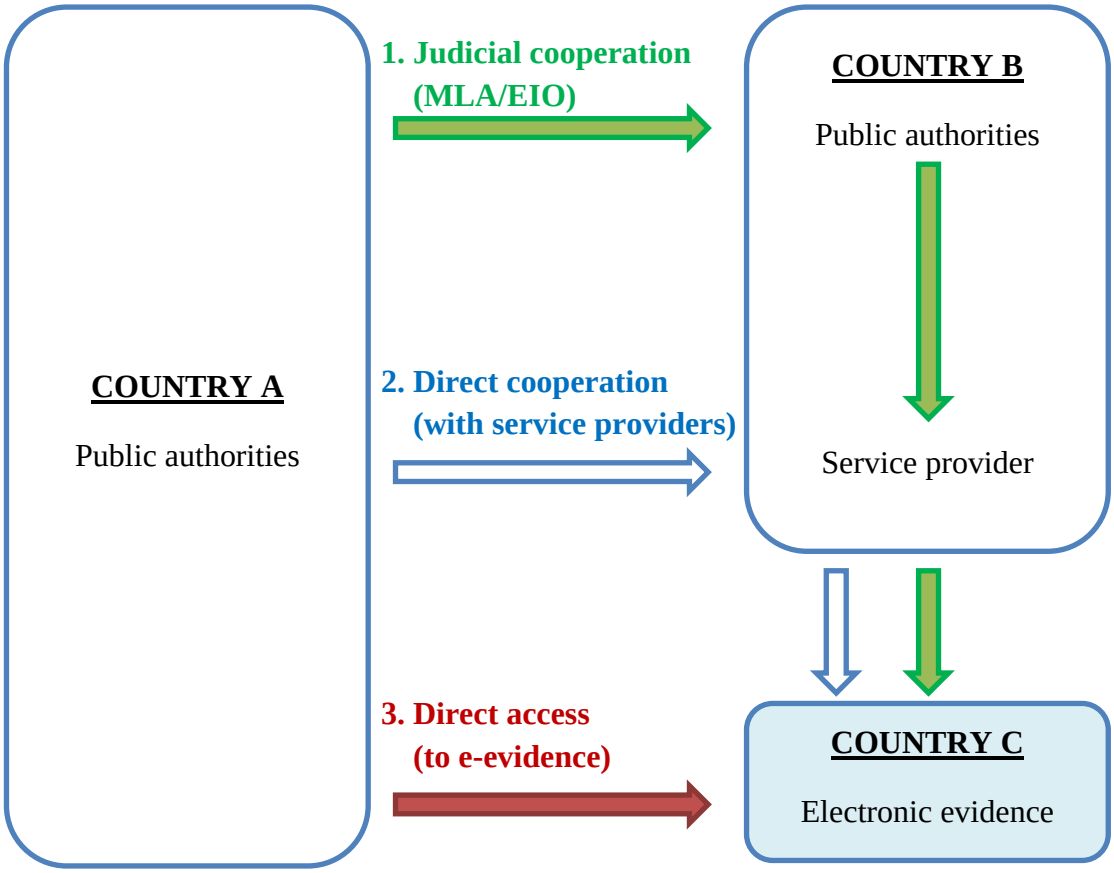
- judicial cooperation is often too slow for timely access to data and can entail a disproportionate expense of resources;
- direct cooperation can be unreliable, is only possible with a limited number of service providers which all apply different policies, is not transparent and lacks accountability;
- legal fragmentation abounds, increasing costs on all sides; and
- the size of the problem is steadily increasing, creating further delays[14].

Figure 1 describes the main parties and channels to access e-evidence across borders today. The main parties are the public authorities requesting access to evidence, the public authorities receiving the request and the service provider that has access to the evidence.

[13] GENVAL Final Report on the Seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime" ("GENVAL Report"), ST 9986/17, p. 52.

[14] See section 2.2.

*Figure 1: the main parties and the three channels for cross-border access to e-evidence*




**1) Judicial cooperation**

- Judicial authorities of country A contact the competent judicial authorities of the country where the service provider is established, formally requesting through judicial cooperation channels (i.e. MLA request or European Investigation Order, EIO) the evidence to which the service provider has access.
- Within the EU, the legal framework on judicial cooperation for obtaining cross-border access to electronic evidence is the EIO Directive. The EIO, based on mutual recognition of judicial decisions, provides for direct communication between judicial authorities rather than going through central authorities, supported by deadlines, standardised forms and limited possibilities to refuse recognition and execution of requests.
- Judicial cooperation with countries outside the EU is mainly based on international agreements, notably the Budapest Convention. Besides that, there are bilateral agreements concluded by the EU (notably, the Agreement with the United States on

mutual legal assistance[15]) and by the Member States, most frequently with the US, followed by Canada and Australia.

**2) Direct cooperation**

- In direct request situations, the public authorities of country A directly contact the service provider established in country B with production orders/requests pursuant to national rules of criminal procedure, and request evidence to which the service provider has access, typically data on a user of the services it provides.
- This concerns some service providers established in the US and, to a more limited extent, in Ireland, which reply directly to requests from Member States' law enforcement authorities on a voluntary basis, as far as the requests concern non-content data.
- For WHOIS data, service providers make data directly available to authorities through a centralised search system which does not rely on individually reviewed requests.[16]

**3) Direct access**

- "Direct access" refers to cases where authorities access data without the help of an intermediary, for instance following the seizure of a device ("extended search") or following the lawful acquisition of login information ("remote search"). The national law in at least 20 Member States empowers authorities, subject to judicial authorisation, to seize and search a device and remotely stored data accessible from it, or to use credentials for an account to access and search data stored under that account. This tool becomes more relevant as data is now regularly stored not on the local device but on servers in a different location, possibly outside of the Member State concerned or even outside of the EU.
- Often, the location of this data is not known to law enforcement (so-called "loss of knowledge of location"), and it may be practically impossible to determine, such as in cases where the data is hosted on Darknet services that use multiple layers of IP relays to disguise their location. As a result, it can be difficult to determine whether such searches have a cross-border component
- Member States have different approaches to direct access and the data storage location (see section 2.2.3).

The requesting public authorities, the receiving public authorities and the service provider, and the e-evidence can all be located in different countries. The general problem that figure 1

[15] Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America.

[16] See Annex 12 for further detail.

describes encompasses multiple specific cases depending on whether each of these countries is located in the EU or not:

*Table 2: mapping of possible situations in cross-border access to electronic evidence*

| **Country** | | | **Comment** |
|---|---|---|---|
| **A**<br>**Requesting public authority** | **B**<br>**Receiving public authority and service provider** | **C**<br>**E-evidence** | |
| EU | EU | EU | Particular case: A=B=C<br>(requesting public authorities, service provider and data in the same country ⇨ national issue) |
| EU | EU | Non-EU | Particular case: A=B<br>(requesting public authorities and service provider in the same country) |
| EU | Non-EU | EU | Particular case: A=C<br>(requesting public authorities and data in the same country) |
| EU | Non-EU | Non-EU | Particular case: B=C<br>(service provider and data in the same country) |
| Non-EU | EU | EU | To be taken into account for potential reciprocity considerations |
| Non-EU | EU | Non-EU | |
| Non-EU | Non-EU | EU | |
| Non-EU | Non-EU | Non-EU | Out of scope |

With regard to the location of the evidence (i.e. country C):

- it is not always known;
- data is volatile and can be moved quickly across borders, so country C can change rapidly, inside and outside the EU;
- data can be split between countries (e.g. data shards, inside and outside the EU);
- there can be copies in multiple countries (inside and outside the EU).

Scope of the problem

The problem affects **all types of data**, from basic information about the subscriber to a given service, to logs showing when a specific user or IP address accessed a service, to metadata and content data. They reflect different levels of **relevance** of the gathered e-evidence: subscriber data is useful to obtain leads in the investigation about the identity of a suspect; access logs can help connect a user to an action; metadata and content data can be most

relevant as probatory material. Challenges affect both access to data at rest (stored data) and to data in transit.

The problem affects **all types of crime that can leave a digital trace:** it is relevant for many types of serious crimes, but also for a number of lower-impact, high-volume crimes such as spreading of malicious software (e.g. ransomware), but also when the only digital element is some form of electronic communication. It is relevant for the gathering of evidence for specific and individual criminal investigations and for specific and limited data access, rather than for other purposes that might require bulk data access.

Most of the relevant information is held by a number of **service providers** including electronic communications service providers and information society service providers, providers of internet infrastructure services and digital marketplaces. Both relevant data and relevant service providers could potentially be **anywhere in the world**, as the relevant services are provided at a distance and are independent of national borders.

In this context, it is important to note that the problems this initiative seeks to tackle have not been created by previous EU instruments. Rather, new technological developments require new answers (and may require them also in the future). The internet is largely privately owned and borderless for everyone except authorities pursuing criminal investigations. States de facto have no control over data as it crosses borders into or from their territory. Accordingly, their purported sovereign interest in maintaining control over any authority's access to that data has been growing more and more limited over time.

This fundamental challenge of data moving swiftly across jurisdictions is unrelated to any existing policy but rather a consequence of the business models of service providers that have evolved organically. The data minimisation principle inherent in data protection laws and the lack of data retention obligations also result in less data being available for shorter periods of time. Data protection rules also create requirements that must be satisfied, e.g. as regards user notification (which arise under the GDPR and the Police Directive).

Size of the problem

It is not possible to determine **exactly** the number of crimes that cannot be effectively investigated and prosecuted in the EU because of challenges in cross-border access to electronic evidence. Data at this level of detail is **not collected** by public authorities. There is no precise data available on the number of requests for judicial cooperation, direct cooperation, direct access or WHOIS lookups.

For **judicial cooperation** requests, based on available data on the European Arrest Warrant and from the European Judicial Network, it can be estimated that there are around **13,000** MLA/EIO requests per year on e-evidence between Member States (including all types of

data). Also, based the figures collected during the 2016 EU-US MLA Review exercise, it can be estimated that the outgoing requests for e-evidence by EU public authorities to the US authorities amount to approximately **1300 per year** (mainly requests for content data).

For **direct cooperation**, the main source of data is the **transparency reports** that some service providers publish concerning the requests they receive from public authorities. The transparency reports do not distinguish whether the request came directly from the Member State in which it originated (direct cooperation request) or it came from the public authorities of a Member State that was asked to cooperate with the one in which the request originated (judicial cooperation request). They concern mostly requests for non-content data.
Given these limitations, the Commission **estimated** the magnitude of the problem, using two main sources of information:

- a **survey** addressed to **public authorities** in Member States[17]; and
- the **transparency reports** from the main service providers (Facebook, Google, Microsoft, Twitter and Apple[18]), which contain information on the number of requests received from public authorities and the percentage of requests fulfilled[19].

The results were broken down in three stages:

1) Percentage of investigations including a **request** to cross-border access to e-evidence.

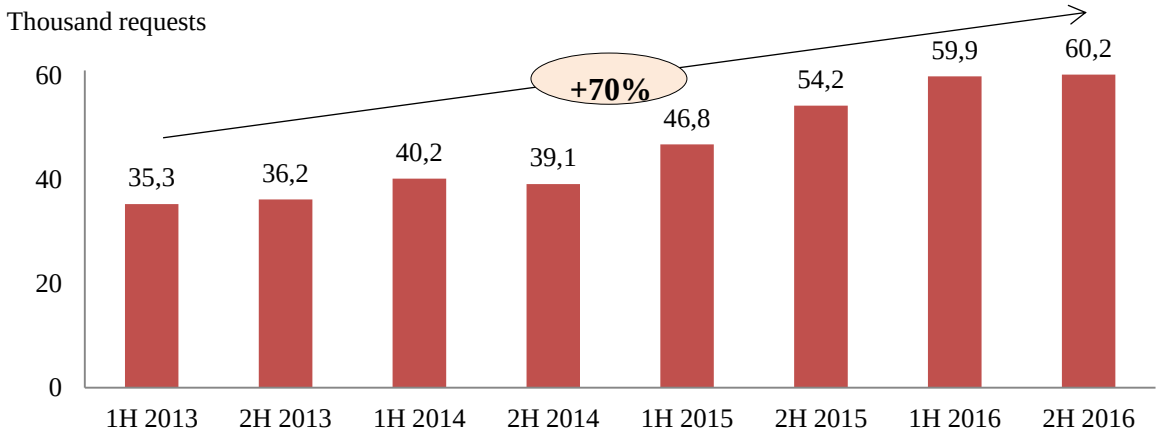
| **More than half** of all investigations include a **cross-border** request to **access e-evidence**. |
|---|

- E-evidence in any form is relevant in around **85%** of total (criminal) investigations.
- In almost **two thirds** (65%) of the investigations where e-evidence is relevant, a request to service providers **across borders** (based in another jurisdiction) is needed.
- Combining the two percentages above results in **55%** of total investigations that include a request to **cross-border access to e-evidence.**
- Requests for non-content data outnumber those for content within the EU and beyond. Non-content data from electronic communications is most commonly requested.

The **transparency reports** provide an idea of the **number** of requests that the above percentages refer to. The figure below shows that the number of requests to the above service providers has **increased by 70%** in the last 4 years:

[17] See Annex 2 for a complete analysis of the survey results. The results presented in this section refer to the median of the responses, to reduce the effect of outliers (sample size = 76 responses).
[18] The transparency reports are available online: Google, Facebook, Microsoft, Twitter and Apple.
[19] It was estimated, that up to 90% of current cross-border requests for non-content data are sent to these five providers, based on their market share.

*Figure 2: evolution of number of Member States' requests[20] to the main service providers[21]*




Other insights from the transparency reports of these providers include (see Annex 11):

- Three Member States, **Germany (35,271 requests), the UK (28,598) and France (27,268)**, accounted for **more than 75%** of the total number of requests from the EU to the five main service providers in the last year.
- **Google and Facebook** accumulated **more than 70%** of the total number of requests from Member States to the five main service providers in the last year.

2) Percentage of requests to **service providers** that are **fulfilled**.

**Less than half** of all the requests to service providers are **fulfilled.**

- The table below summarises the responses to the **survey** of public authorities in Member States on the percentage of investigations where the request to service providers was fulfilled, using judicial and direct cooperation channels.
- The table shows that the requests for **content** are comparatively the **most difficult** to fulfil and the requests for **subscriber data** the least difficult to fulfil, regardless of whether the requests is within the EU or with non-EU countries. Nonetheless, even the requests for subscriber data remain unfulfilled in a significant percentage of cases, more than half for requests to non-EU countries, which are particularly relevant, as shown in point 1) above.

[20] Indicated growth of 70% corresponds to annual growth rate (CAGR) of 14% over the 2013-2016 period.

[21] Includes standard and emergency access requests for these service providers except Apple, where only standard requests are included (Apple's transparency reports only include emergency requests since 2015 and they only report on emergency requests answered since July 1 2016). The transparency reports of Google and Apple do not differentiate between preservation requests and standard and emergency requests until 30 June 2014 and 31 December 2014 respectively. Apple's device-based requests are not included. See Annex 4 for the complete data compiled from the transparency reports used in this section.

- The table shows that the requests for access to e-evidence **within the EU** are comparatively fulfilled **more easily** than **with non-EU countries**, regardless of the type of data.

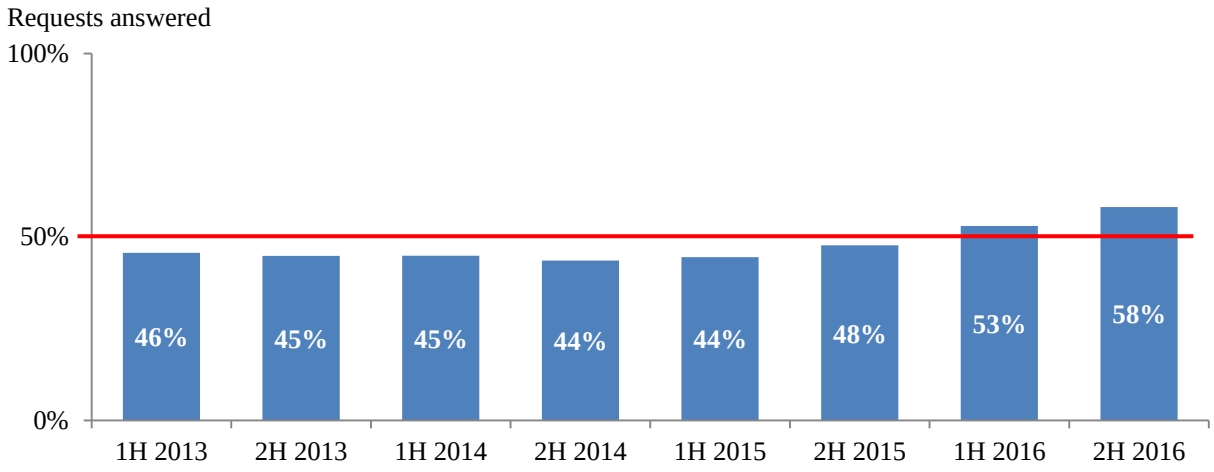
*Table 3: percentage of requests to service providers that are fulfilled (survey data)*

| | | Within the EU | | With non-EU countries | |
|---|---|---|---|---|---|
| | | Judicial | Direct | Judicial | Direct |
| Non-content data | Subscriber data | 75% | 55% | 45% | 45% |
| | Metadata | 60% | 45% | 35% | 35% |
| Content data | | 55% | N/A[22] | 30% | N/A[23] |

- The median of the above responses is **45%.**

The **transparency reports** include data on the requests from the Member States that are answered, so it is possible to compare this data with the one from the survey:

*Figure 3: evolution of the % of requests from Member States answered by service providers*




- The graph above shows that the response rate has remained **under 50%** in the 2013-2015 period and was more than 50% only in 2016.

[22] Direct cooperation with service providers for access to content data is usually available for emergency situations only, which represent a very small number of total requests. Although the survey did not provide for sufficient granularity to indicate whether a request was related to an emergency situation many of the respondents to this question came from counterterrorism units or were otherwise involved in serious crime areas that typically may give rise to emergency requests. Follow-up calls with individual respondents supported this assessment.

[23] *Ibid.*

- The transparency reports contain information on the number of requests **answered**, which might not be necessarily the same as **fulfilled.** The percentage of requests fulfilled is likely to be **lower** than the percentage of requests answered.
- The number of outgoing MLA requests to the US is still much smaller than the number of unsuccessful direct cooperation requests. This means that in case a direct cooperation request is unsuccessful, it is only rarely followed-up by a MLA request. In these situations, the evidence will not be available for the investigation.
- The period 2013-2016 is likely to have shaped the most the perception of public authorities and their responses to the survey. The median of the percentage of requests answered by service providers in the 2013-2016 period is **45%**, which is indeed the **same estimate** obtained in the survey.

The transparency reports and the targeted survey to Member States indicate that a request could remain unfulfilled for a variety of reasons, including that the request is sent to a provider who does not hold the data, it is excessively broad or unclear, it fails to specify an (existing) account or sought information, it does not have a valid legal basis or the data sought no longer exists.

3) Percentage of crimes involving cross-border access to e-evidence that **cannot be effectively investigated or prosecuted**.

Almost **two thirds** of crimes involving cross-border access to e-evidence **cannot be effectively investigated or prosecuted.**

- The table below summarises the responses to the **survey** on the percentage of investigations involving requests to access e-evidence across borders that are negatively affected or cannot be pursued:

*Table 4: percentage of investigations involving requests to access e-evidence across borders that are negatively affected or cannot be pursued*

| | Within the EU | | With non-EU countries | |
|---|---|---|---|---|
| Cause | Judicial | Direct | Judicial | Direct |
| Lack of timely access[24] | 35% | 25% | 45% | 15% |
| Lack of access (access denied) | 25% | 25% | 25% | 15% |
| Other | 15% | 5% | 15% | 10% |
| **Total** | **75%** | **55%** | **85%** | **40%** |

[24] I.e. data not provided in time, causing e.g. the disappearance of other leads.

- The table shows that the **lack of timely access** is more significant when using **judicial cooperation** channels, in particular **with non-EU** countries.
- Direct cooperation seems to be a more efficient channel than judicial cooperation, in particular with service providers based in non-EU countries. Since this channel is based on **voluntary** cooperation, public authorities indicated that they tend to limit their direct cooperation requests to the service providers that **they know** are willing to cooperate, which might also explain the relatively low percentage of investigations negatively affected. In the rest of the cases, judicial cooperation is the only channel left to request access to data across borders, which might also explain the higher percentage of investigations negatively affected.
- In addition, direct cooperation is typically limited to non-content requests, whereas judicial cooperation includes also content requests, which are more problematic (see the problem drivers in section 2.2.).
- The median of the above responses is **65%**: almost **two thirds** of crimes[25] involving cross-border access to e-evidence **cannot be effectively investigated or prosecuted.**

### 2.1.2. Cross-border dimension

This initiative covers a variety of crimes with an increasing cross-border dimension. To illustrate this, consider Hans, a German prosecutor who has to deal with cases such as[26]:

- Terrorism: after a terrorist attack in **Germany**, the German police find connections of the suspect terrorist to a cell that has been involved in other terrorist attacks in **France, Belgium and Spain**. The suspect has spent time in **Syria, Turkey and Morocco**. The German police have indications that the terrorists communicated through email drafts: one terrorist drafted an email and instead of sending it, saved it to the draft folder, accessible online from anywhere in the world. The other terrorist opened the same account and read the message. As the email was never sent, it was not possible to track. The Microsoft server hosting the account is in **Ireland**. Hans prepares an MLAT request to the Irish authorities in order to gather more information about the suspect terrorist's email account contents.
- Child sexual abuse: after having infiltrated a website for exchanging child sexual abuse material in the Darknet for more than a year, the **Australian** police have gathered information on more than one million users **globally**, which they have started to distribute to law enforcement **around the world**. Some of the child victims appear

[25] The number of investigations is used as a proxy for the number of crimes. An investigation could include several crimes so the estimates for the number of crimes are likely to be on the conservative side.

[26] Hans is a fictional name. Also these cases are partially fictional but nonetheless representative of the daily work of public authorities, as described during the stakeholder consultation.

to be in **Germany**. The investigation has revealed the offender's Facebook profile; Hans prepares a production request (direct cooperation) to Facebook (based in the **US**) in order to gather more information about the possible offender's exact location using his Facebook account.

- Human trafficking: a **Syrian** national is arrested in Germany, near the Austrian border, accused of human trafficking. The suspect was taking advantage of the refugee crisis to facilitate illegal border crossing from Turkey to Germany through the Balkan route (**Turkey, Greece, Former Yugoslav Republic of Macedonia, Serbia, Croatia, Slovenia, Austria and Germany**). The smart phone of the human trafficker was seized by the German police. It contains not only the contact information of other members of the criminal organisation he belongs to, but also indications that the human trafficker used WhatsApp. Although the WhatsApp conversations were deleted from the phone, a backup exists in **the cloud,** accessible via the seized mobile device. The German police, under Hans' supervision, directly access these conversations to dismantle the organised crime network.
- Cybercrime: a network of millions of infected computers worldwide is controlled by a central server (a so-called "command and control" server) and used to distribute spam and malicious software, such as ransomware and spyware, on victims' computers. The command and control server moves from one domain to the next every five minutes, **without regard to national boundaries**. In a first investigative step, Hans and his colleagues search the domain name WHOIS system to obtain information on the owners of the domain names used by the command and control server.

Even crimes that may appear as having no cross-border dimension can actually have one because of e-evidence. Consider for example an assault case in which a **German** national assaults a **German** victim in **Germany**. Hans investigates the case and arrests a suspect. A witness has doubts when asked to identify the person arrested, but reports that she saw the perpetrator made selfies of himself and the assaulted victim lying on the ground with his mobile. Hans confiscates the suspect's phone but finds no relevant pictures on the mobile. The suspect had installed Dropbox and had secured it with a password. Hans needs access to those pictures which, he knows, are stored in the **US**. He prepares an MLA request to the US, as the German legislation does not allow him to access directly that data in the US.

In general, crime has an increasing cyber component, and with it an increasingly prominent cross-border dimension. Whereas the data storage location is still considered as a relevant factor to assert jurisdiction, it is determined for the vast majority of cases by the provider alone, on the basis of business considerations. This choice makes cross-border cooperation necessary in cases which may have no other connection across borders.

### 2.1.3. Why is it a problem

The fact that some crimes cannot be effectively investigated and prosecuted in the EU is a problem because it results in criminals enjoying impunity, victims being less protected and EU citizens may feel increasingly threatened by criminal activity[27]. In general, it hinders the accomplishment of an area of **freedom, security and justice** in the EU.

In particular, when some crimes cannot be effectively investigated and prosecuted because of challenges in cross-border access to e-evidence, there are negative consequences at all stages:

1. **Before** the crime is committed: when electronic evidence is difficult to obtain across borders the perception of impunity is reinforced.
2. **While** the crime is being committed: when a crime is ongoing and public authorities are investigating it, effective and timely access to electronic evidence can save lives or prevent serious damage. For example, in terrorism cases with hostages or in ongoing child sexual abuse situations, the time that law enforcement requires to get to the victims can determine whether they survive or not.
3. **After** the crime has been committed: electronic evidence is volatile and can be transmitted, altered or deleted easily. Public authorities therefore need effective and timely access to it to be able to prosecute criminals and prevent future crimes. There are no mandatory data retention rules in the US (where some of the most important service providers are based) or at EU level, since the Data Retention Directive[28] was declared invalid by the European Court of Justice in 2014[29]. At the same time, data minimisation requirements force service providers to delete data more quickly. This contributes to the volatility of e-evidence and reinforces public authorities' need for timely access in criminal investigations. Timely access is also important as investigations often have to proceed step by step, identifying first leads and then following further indications provided by those leads, which often necessitate repeated, iterative requests for access to electronic evidence across different service providers and jurisdictions. If the first requests are fulfilled slowly, the chances to find any data in response to further requests decrease significantly.

---

27 Special Eurobarometer 432 'Europeans' attitudes towards security' and Special Eurobarometer 464a 'Europeans' attitudes towards cyber security' suggest that EU citizens feel increasingly threatened by terrorism, cybercrime and organised crime.

28 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

29 ECLI:EU:C:2014:238 (case C-293/12, Digital Rights Ireland Ltd v Minister for Communications). The Tele2/Watson case of December 2016, ECLI:EU:C:2016:970 (case C-203/15, Tele 2 Sverige), provided additional guidance on the rules around the retention of communications data and the safeguards that must be in place to protect it.

### 2.1.4. Who is affected and how

The following parties are affected by the challenges in cross-border access to e-evidence in criminal matters:

- **Society** in general: the fact that some crimes cannot be effectively investigated and prosecuted in the EU damages the secure environment and the effective application of the rule of law required for a society to thrive.
- **Victims** of crime (natural and legal) suffer the negative consequences (e.g. economic, physical, psychological) of a delayed (or even an impossible) investigation and prosecution of the crime they have become victims of.
- **Suspects** in criminal investigations: the procedures that regulate cross-border access to electronic evidence must provide legal certainty, transparency, accountability and respect of fundamental rights and procedural guarantees of the suspects in criminal investigations.
- **Users** of the services offered by service providers: the procedures that regulate cross-border access to electronic evidence must provide legal certainty, transparency, accountability and respect of fundamental rights of the users of the services offered by service providers, to the extent that they may become part, inadvertently, of a criminal investigation.
- **Service providers:** as the parties with access to electronic evidence, they receive requests to access e-evidence from public authorities, either directly or through MLAT procedures. They invest resources in responding to those requests, which can be significant as the number of requests keeps increasing and the framework to regulate cooperation with public authorities has room for improvement.
- **Public authorities** (judiciary, law enforcement) from the country issuing the request: they require access to e-evidence to investigate or prosecute crimes. Often, electronic evidence is the only significant lead for investigators, so without access to that evidence the investigation may have to be abandoned, with the negative consequences that this brings for the victims, future victims and society at large, due to the perception of impunity and the weakening of the rule of law.

  Public authorities from the country receiving the MLAT request are also important parties in this process. As MLAT requests are likely to keep on increasing, the improvement of the current procedures is important so that they can fulfil the requests for cooperation in a timely and effective manner.

## 2.2. What are the problem drivers?

The three problem drivers identified are:

1. It takes **too long** to access e-evidence across borders under existing **judicial cooperation** procedures, rendering investigations and prosecutions less effective.
2. Inefficiencies in **public-private cooperation** between service providers and public authorities hamper effective investigations and prosecutions.
3. Shortcomings in defining **jurisdiction** can hinder effective cross-border investigations and prosecutions.

The following sections summarise the analysis of the problem drivers. A deeper and more detailed analysis is available in Annex 6.

### 2.2.1. It takes too long to access e-evidence across borders under the current judicial cooperation procedures, rendering investigations and prosecutions less effective

Judicial cooperation procedures were designed to ensure respect for the sovereignty of foreign countries on whose territory an investigative or enforcement action needed to be performed. Usually there was a substantial connection to that territory. This substantial connection has become increasingly virtual in the context of e-evidence. Sometimes, the data storage location in a server park or the establishment of a service provider is the only factor connecting an investigation to a given foreign country.

In many cases, data is no longer stored on a user's device but made available on cloud-based infrastructure for access from anywhere. Service providers do not need to be established or to have servers in every jurisdiction but rather use centralised systems to provide their services. Cross-border requests have multiplied accordingly, resulting in increased delays in responses. At the same time, data minimisation requirements lead to shorter data storage periods for some types of data; delayed requests risk not finding any data left.

In parallel, a number of countries are questioning the appropriateness and usefulness of mutual legal assistance procedures in these circumstances, especially when it comes to less sensitive data categories. Some have not invested sufficient resources to keep up with the growth in foreign demand, given that there is no own interest in the relevant investigations and the service is provided out of courtesy to the foreign country. This has further contributed to the delays in responses.

Within the EU

The EIO Directive, in application since May 2017, covers the **gathering and transfer of evidence** between Member States, based on **mutual recognition** of judicial decisions. The EIO Directive provides for **deadlines of 120 days** (30 days for the executing authority to make a decision on the recognition or execution of the EIO and 90 days to carry out the investigative measure[30]), which is faster than the MLA procedure. This improvement is still considered **insufficient** by Member States' experts for accessing e-evidence in criminal investigations, for which the EIO process would still be too long and therefore ineffective.

The time for accessing electronic evidence is a crucial factor in any investigation:

1. In the absence of retention obligations, providers have no incentive to store data – in particular metadata – for longer than necessary. Data storage is a cost factor.
2. The data minimisation principle inherent in data protection rules obliges providers to store data only for as long as it is necessary.
3. Investigations proceed in an iterative manner. In a typical case, an authority might first contact a service provider to obtain an IP address used to access a service, then turn to the internet access provider to determine who used that IP address at the relevant point in time. If the first step takes more than a few days, then the information on who used the IP address will most likely have been deleted already.

In certain cases the EIO Directive allows for shorter time-limits. The issuing authority can indicate in the EIO that a shorter deadline is necessary "due to procedural deadlines, the seriousness of the offence or other particularly urgent circumstances" (cf. Art. 12(2)). Article 32(2) provides for a 24-hour deadline to decide on provisional measures. Nevertheless, these shorter deadlines cannot address the specific needs of e-evidence with its high relevance for criminal investigations: the first is an exception rather than the general rule, requiring reasons for urgency in every case, and the second is specifically aimed at preservation of the data only. Preservation of data alone would not solve the issue: timely access is important as outlined above.

Requests for mutual legal assistance (currently up to 5000 per year[31]) and for recognition and execution of the EIO, follow-up correspondence and enquiries for information are often still sent by traditional means, i.e. by post or fax, contributing to the time the current process takes.

All Member States participate in the EIO Directive except Ireland and Denmark, which continue to rely on MLA channels[32]. For Ireland, where a number of service providers have

[30] See Article 12 of the EIO Directive on time limits for recognition or execution.
[31] E-CODEX, Criminal Justice – Mutual Legal Assistance, on MLA requests in all areas, not only e-evidence.

their European headquarters, stakeholders have reported an increase in the time needed to access e-evidence, presumably due to the high number of requests to Irish authorities. Since the EIO deadlines do not apply, this increase might continue to grow.

The problem to access electronic evidence has become so pressing that despite the imminent entry into force of the EIO Directive, the Council has repeatedly called upon the Commission in 2016 to take action.

With non-EU countries

The main legal instruments that Member States use to request access to e-evidence stored in non-EU countries are MLA requests. These formal procedures ensure that the right authorities are involved and that appropriate safeguards are taken into account in both countries when there is a sovereign interest of more than one country. The procedures were designed at a time before the internet, when volumes of requests were a fraction of today's, and are ill equipped to handle today's numbers[33]. In addition, the legal framework for mutual legal assistance is fragmented and complex: practitioners are faced with a high number of bi-lateral and multi-lateral conventions and have to ensure compliance with the specific requirements of recipient countries' legal systems that they are often less familiar with (e.g. probable cause in the US, as will be explained below).

*Box 1: judicial cooperation on e-evidence*

Judicial cooperation requires a significant investment on the part of both the requesting and the receiving countries.

- On the side of the **requesting country**, besides the requirements of the domestic procedural and substantive laws, the specific conditions of the judicial cooperation instruments and the foreign law have to be met; translations need to be obtained, and a significant number of formal approvals have to be granted.
- The **receiving authority** has to check the validity of the request and the absence of any obstacles under national law, and then use the necessary national tools for enforcement. The receiving country regularly has to make this investment without any own interest in the solving of the case at hand, based on a spirit of mutual cooperation and on the assumption that the same courtesy

[32] For example, Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union; European Convention on Mutual Assistance in Criminal Matters (CETS No.030); and other bilateral or multilateral agreements.

[33] The T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, adopted by the T-CY at its 12th Plenary (2-3 December 2014), also concludes that current mutual legal assistance procedures are considered too complex, lengthy and resource intensive, and thus too inefficient, p. 123.

would be afforded in return by the country that is now requesting, if roles are reversed. However, in particular in cases relating to e-evidence, this balance of *mutual* legal assistance has become **skewed**, as the dominant service providers congregate in a small number of jurisdictions. As a result, these countries receive a disproportionate volume of requests that can outnumber their own outgoing requests by a factor of 10, as is the case for the US.

The main recipient of MLAT requests from Member States (and from around the world) for access to e-evidence is the US, where the largest service providers are headquartered. This is why the impact assessment focuses on the US situation, but many of the structural problems of MLA cooperation are similar when it comes to other non-EU countries. In many cases, the requests received have little or no connection to the US besides the seat of the service provider. This forces US authorities to provide thousands of full checks for cases, giving them essentially the same attention as domestic cases, in the absence of any specific US interest in the solving of that concrete crime.

The MLAT process with the US takes an average of **10 months**[34], which is considered as **too much time** by all stakeholders. There have been repeated calls for reform within the stakeholder consultation for this initiative and before[35].

There were extensive consultations in the EU and the US to determine the reasons that explain the long duration of the MLAT process. The stakeholders identified the **high volume of requests** to access e-evidence as the main factor that has put the MLAT system under enormous strain, and has shown its weakness to deal effectively with the current needs. The number of requests has increased 10 fold over the last decade, reaching around 1600 MLA requests from around the world last year, most of which come from the EU.

Other reasons that the stakeholder identified are:

1. **Quality** of the request, which can make the response time vary significantly. The higher the quality, the fewer the iterations required between the two countries, and the

[34] Daskal, Jennifer, A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right, February 2016.

[35] Examples of recent calls for reform from the U.S. include:

- Vivek Krishnamurthy, Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal Assistance Treaty System and Why It Matters, Berkman Klein Center Research Publication No. 2016-3, February 2016;
- Jonah Force Hill, Problematic Alternatives: MLAT Reform for the Digital Age, Harvard National Security Journal Online, January 2015;
- Global Network Initiative, Data Beyond Borders: Mutual Legal Assistance in the Internet Age, January 2015;
- Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, December 2013.

faster the process can be. The most common issue is unclear **probable cause** (e.g. the connection between the criminal activity and the account) for requests for content and other missing information such as the **timeframe** relevant to the e-evidence sought.

2. **Type** of request: the requests for **content** take much longer than the requests for non-content, as the former require higher standards such as proving probable cause and undergo more complex procedures such as search warrant and filtering or data minimisation (review of all the content to determine what is relevant to the offence and can be forwarded to the requesting country).
   **Emergency** requests usually can be answered effectively, within 24h. The problem is that authorities in the EU are unfamiliar with the mechanism[36].
3. **Service providers' internal procedures**. The time that a service provider takes to process a request varies depending on its internal procedures. Member State authorities pointed out the **lack of transparency** of these procedures.

### 2.2.2. Inefficiencies in public-private cooperation between service providers and public authorities hamper effective investigations and prosecutions

Given the limitations of the judicial cooperation channel described above, Member States regularly obtain **non-content** data through direct cooperation with service providers on a **voluntary**[37] basis. This option is supported by the US Department of Justice (DOJ) as the preferred one, as evidenced by letters from the DOJ to Member States. Direct cooperation has become the main channel for authorities to obtain **non-content** data, as both authorities and service providers acknowledged during the consultations, and as reflected by the significant number of this type of requests (more than **120 000** in 2016)[38].

This section analyses the inefficiencies in this type of public-private cooperation, which prevent direct cooperation from being a fully satisfactory solution.

Within the EU

In close to all EU Member States, the telecommunications framework prohibits national telecommunications providers from responding directly to requests from foreign authorities. In addition, there is no legal framework allowing direct cooperation in other communication sectors. Therefore, it is rare to non-existent and mainly used in emergency situations. Only

---

36 18 U.S.C. § 2702(b)(8).

37 "Voluntary" means that there is a domestic legal title which cannot be enforced directly in the recipient country. Nevertheless, the distinction between voluntary and mandatory cooperation is not always easy to establish, and in fact, in the absence of a clear legal framework the parties involved may disagree on the voluntary or mandatory nature of the direct cooperation.

38 Based on the 2016 transparency reports by Google, Facebook, Microsoft, Twitter and Apple.

service providers based in Ireland provide **non-content** data on a **voluntary** basis. When public authorities address requests for direct cooperation to US service providers operating in the EU, unless the service providers are based in Ireland, they typically get redirected to the US, where the service provider holds the data or where the management of these requests within the company takes place.

With non-EU countries

Given the inefficiencies of the current MLA procedures, the 2016 Review Report of the EU-US MLA Agreement encouraged Member States to cooperate directly with US service providers in order to secure and obtain e-evidence more quickly and effectively. This approach is actively supported by US authorities, as mentioned above.

The US law that allows US based service providers to cooperate directly with European public authorities[39] with regard to **non-content data**[40] is section 2701(2) of the Electronic Communications and Privacy Act 1986 (ECPA)[41]. This cooperation is **voluntary**[42]. Thus, providers have created their own policies or decide on a case-by-case basis on whether and how to cooperate. The analysis below reflects the main concerns raised by stakeholders from their various perspectives. It necessarily abstracts from companies' individual policies and procedures and may therefore not apply to all situations in an identical manner[43].

Stakeholders expressed general and practical concerns:

- General:
    1) transparency of the process;
    2) reliability of stakeholders;
    3) accountability of stakeholders;
    4) admissibility of evidence;
    5) unequal treatment of Member States;
    6) reimbursement of service providers' costs;

[39] The five year review carried out in 2016 of the EU-US MLA agreement also contained recommendations for Member States to seek to obtain direct cooperation from US-based service providers in order to secure and obtain e-evidence more quickly and effectively.

[40] Given that it is a voluntary system from the perspective of US laws, each provider decides what kind of non-content data would be disclosed following a direct request from law enforcement authorities in the EU.

[41] As described in annex 6 (Box 1), ECPA prohibits service providers to give access to content data on a voluntary basis, except in cases of emergency.

[42] The cooperation is voluntary from the perspective of ECPA, even though law enforcement in some Member States may be using nationally binding orders in making the request.

[43] For a more company-specific analysis see e.g.: Council of Europe Budapest Convention on Cybercrime Convention Committee (T-CY), Criminal justice access to data in the cloud: Cooperation with "foreign" service providers, T-CY (2016)2, provisional document of 3 May 2016.

- Practical:
    7) for authorities, how to identify and contact the relevant service provider;
    8) for service providers, how to assess authenticity and legitimacy of requests.

Annex 6 contains a detailed analysis of each of these concerns.

### 2.2.3. Shortcomings in defining jurisdiction can hinder effective cross-border investigation and prosecution

The previous two drivers have shown, respectively, the challenges that the judicial cooperation and direct (voluntary) cooperation with service providers present for Member States when trying to access e-evidence across borders. These challenges prevent these channels from working properly and being sufficient to address the current needs.

In the face of these challenges, Member States have developed two mechanisms to define their jurisdiction over the e-evidence and try to access it across borders:

1) **Domestic production orders**, in which the Member State asserts jurisdiction through various **connecting factors** over the data held by a service provider and mandates it to release the data.
2) **Direct access** to data, in which the Member State asserts jurisdiction over data for which it is not possible to determine its location, and accesses it directly from an information system within its territory, without the assistance of an intermediary (e.g. a service provider or other public authorities).

These measures are partially grounded in the conviction, apparent throughout the expert consultations, that a case presenting no links to the country/countries where the service provider has its main seat or where it has chosen to store the relevant data does not necessitate (full) involvement of that country's authorities.

1) <u>Domestic production orders: connecting factors</u>[44]
   A fundamental challenge highlighted by stakeholders across all three channels to access electronic evidence lies in the fact that stakeholders and legal frameworks disagree as to **what constitutes a "cross-border" situation,** which makes it difficult to determine when a country can exercise jurisdiction.

[44] A connecting factor is a fact that connects an occurrence with a particular law or jurisdiction. Examples include the place where a crime was committed, the nationality of the suspect or the place where a legal person is registered. In the area of cross-border access to e-evidence, a connecting factor is a fact that can be used to determine whether a country can apply a certain law or exercise jurisdiction that allows it to mandate, access or request access to e-evidence.

Based on the results of a questionnaire to Member States, the most common **connecting factors** used include:

- the storage or processing location of the data[45] (i.e. where the infrastructure used for the storage or processing of the data is located) [46]. While most Member States' laws attach importance to the storage location of the data, this has proven very difficult in practice as a connecting factor (e.g. while Facebook operates a large data centre in northern Sweden, Sweden has always been asked to send its request to Facebook's headquarters in the United States). As a result, there has been a trend to move away from data storage location in several Member States and internationally[47]. This is also the preliminary result of a global multi-stakeholder exercise to determine principles for cross-border access to data[48];
- the location of the seat of a service provider;
- the place where a service provider has any another establishment;

---

45 While data location is often cited as a key factor in determining territorial competence, in practice it is impossible for authorities to tell where the data is stored without the cooperation of service providers. Therefore authorities can only direct mutual legal assistance requests at a given country once the service provider has disclosed the data storage location and has agreed to keep the data in place, i.e. not to move it to another jurisdiction. Service providers may also choose to "shard" their data, storing bits in various locations, and some have internal technical measures and policies allowing access to data only from one country regardless of whether it is stored there or – wholly or in part – in other countries. See U.S. District Court for the Eastern District of Pennsylvania, In re Search Warrant No. 16-960-M-01 to Google, p. 7 and 8, for further details.
In relation to data location see also U.S. Court of Appeals for the Second Circuit, Microsoft v. United States, No. 14-2985 (2d Cir. 2016) of 14 July 2016. The case is under review by the U.S. Supreme Court and a decision is expected by July 2018. See Annex 9 (Box 1) in this document for more details.

46 The data storage location depends on business considerations designed to ensure swift access for users and secure a resilient system architecture. Location may shift multiple times within a short period. Where storage location is not an explicit part of the business model – such as for some corporate customer solutions - it often does not coincide with the place where the user is using the service. The use of specific storage algorithms for data stored in the cloud makes it very difficult in some cases to determine the storage place; not even the service provider may be able to provide the necessary information in due time.
In addition and for reasons of data security, data in the cloud is often split. For example, Microsoft has currently more than 100 data storage centres in more than 40 countries across the world, and pieces of the requested data could be found in several of those. Some service providers change the data storage location of all data automatically within a few days or even a shorter period. Thus, even if the service provider could tell where the data was at a certain point of time, the information could be outdated by the time it reaches the requesting authority.
At the same time, service providers must be able to locate the data (and thus to know its location) as specific obligations apply to the data depending on where it is stored and/or further processed (e.g. data protection rules). From a commercial point of view, it should also be noted that an increasing number of service providers are marketing to customers the fact that their data will stay in the EU.

47 The ongoing negotiations in the T-CY Committee, the Committee representing the Parties to the Council of Europe Budapest Convention on Cybercrime, on a second additional protocol to the Budapest Convention, include the aim to move away from data storage location as a decisive factor.

48 Internet & Jurisdiction, Data & Jurisdiction Program: Cross-Border Access to User Data, May 2017.

- the place where a service provider is offering services[49];

Other connecting factors that have been considered include the nationality of the suspect and the nationality of the victim[50].

The use of different connecting factors not only creates **legal uncertainty** for authorities, but also for service providers receiving the requests. In particular, service providers active in multiple countries highlighted during the consultations **conflicting regulations** of those different countries. It is not always obvious to the service providers which legal regime applies and at times the service providers might be unable to produce data due to conflicting laws between countries[51]. As a result, service providers called for a more streamlined process, facilitating lawful access to data in ways that ensure protection of fundamental rights, and reducing situations where they are faced with conflicting rules[52]. As it is unclear to what extent a service provider is obliged to respond to a request based on different connecting factors, the legal uncertainty may also interfere with **rights of the persons** to which the requested evidence relates, including their right to privacy. A number of legislative instruments even employ different connecting factors depending on the **type of e-evidence**, usually granting larger domestic competences for non-content data than for content data. At the same time, there is **no common understanding** of how to categorise the specific types of e-evidence[53]. For example, while some service providers consider the IP address used at the time of creation of an account as basic subscriber information, others view it as transactional data. Other types of electronic evidence for which no legal definitions are available may also be of relevance for criminal

---

49 See e.g.: Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N of 1 December 2015, and Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12 of 27 October 2016.

50 See e.g.: Conings, C., Locating criminal investigative measures in a virtual environment, 2014; see also Discussion paper on tackling cybercrime, Informal Meeting of the Justice and Home Affairs Ministers, Amsterdam 25-26 January 2016.

51 See e.g.: Mike Masnick, Brazil Arrests Facebook Exec Because Company Refuses to Reveal Info On WhatsApp Users, Techdirt, March 16, 2016.

52 See e.g.: RGS Statement on US-UK Data Protection Discussions, July 15, 2016.

53 In the targeted survey 1 of September 2016, 12 Member States indicated that they use a definition of subscriber information (AT, RO, SE, EL, LV, DE, DK, ES, FI, PT and UK), 15 Member States indicated they use a definition of traffic information (AT, RO, SE, BE, SK, EL, LV, DE, DK, ES, FI, PT, SI, UK and LT), and 8 Member States indicated they use a definition of content information (AT, RO, EL, DE, DK, ES, FI and FR). These definitions, sometimes based in international conventions or EU acquis, are not the same across Member States. This problem is also highlighted in the GENVAL Final Report on the Seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime" ("GENVAL Report"), ST 9986/17, p. 49.

investigations, including data unrelated to communications. All of these categories may contain personal data[54].

The absence of certainty as to which data category applies can lead to an **uneven application of procedural safeguards**, as legal procedures and safeguards vary across different categories of e-evidence. It may also result in conflicts of law as regards the scope of measures. At a more practical level, it may lead to misunderstandings between requesting authority and executing authority or service provider addressed.

In general, the use of different connecting factors in different countries can be an obstacle to cross-border investigations and prosecutions and create tensions between countries.

The use of different connecting factors and the resulting challenges led the Parties to the Council of Europe Budapest Convention on Cybercrime to initiate discussions on an **additional protocol** to the Convention (see policy measure 3 in section 5).

Although the use of the approaches outlined above to address cross-border situations may provide for a domestic legal mandate for direct cooperation of a service provider, it does not necessarily provide for effective means to oblige a service provider to execute it. Despite a few court decisions[55] about the obligations of service providers, **execution in case of non-compliance** remains a challenge unless the service provider is established in the relevant country. National authorities rely on conventional enforcement mechanisms, including issuing fines and criminal penalties at national level where non-compliant service providers are located in another country. They also may rely on the country where the relevant service provider is established to ensure the execution of the domestic production order, using MLAT, which contradicts the original intention behind the use of a domestic production order (i.e. to be an alternative to MLAT procedures).

For the specific case of WHOIS data that is made available by service providers through a credentialed-access system, domestic legislation might not provide for this possibility. Stakeholders highlighted the importance of swift access for investigative purposes. One head of a Member State national cybercrime unit estimated that his team alone makes around 50,000 WHOIS look-ups per week.

---

54 Personal data is any information related to an identified or identifiable natural person, as defined in Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

55 See e.g.: Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N of 1 December 2015, and Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12 of 27 October 2016.

*Box 2: The Domain Name WHOIS System*

> The term **"WHOIS"** refers to a system of databases that provide information on who owns a domain name. Every year, millions of individuals, businesses, organisations and governments register domain names. Each one must provide **identifying and contact information** which may include: name, address, email, phone number, and administrative and technical contacts. A large part of the WHOIS is currently publicly available, e.g. via WHOIS.icann.org, but a number of registries already operate closed systems using credentialed access. In the course of ensuring compliance with data protection principles, this trend is likely to expand to the remaining WHOIS system (see Annex 12).

2) Direct access to data: asserting jurisdiction

For direct access to e-evidence, public authorities require no technical help from a service provider or other public authorities. Data is now regularly stored not on the local device but on servers in a different location, possibly outside of the Member State concerned or even outside of the EU, possibly using dynamic storage systems and rotating locations. Often, it is neither feasible nor possible for an authority to determine the location of the data (i.e. "loss of knowledge of location" or "loss of location").

*Box 3: What is **loss of location** and why does it matter?*

> "Loss of location" refers to a situation where law enforcement cannot establish the physical location of the perpetrator, the criminal infrastructure or electronic evidence. In the case of data, the growing use of cloud-based storage and services means that data stored in the cloud could be physically located in different jurisdictions[56]. Furthermore, recent trends such as the Darknet have contributed to facilitate hiding data location[57].

In these situations, when law enforcement has access to the data without knowing its precise location, there can be a risk of losing it as it may be moved or deleted. Also, when the data subject is made aware of the investigation, as is typically the case for an open search measure, he or she can delete the data from another device within seconds. In addition, the circumstances of a particular investigation may not allow timely determination of the

[56] Data sharding – the storage of different parts of a database across various servers that might be in different physical locations – has become a common security technique. See footnotes 45 and 46.

[57] See e.g.: Discussion paper on tackling cybercrime, Informal Meeting of the Justice and Home Affairs Ministers, Amsterdam 25-26 January 2016;
See also Europol Internet Organised Crime Assessment (i-OCTA) 2017.

location of infrastructure for the storage or processing of e-evidence, for instance in emergency situations.

Based on the responses to a questionnaire (targeted survey 1), Member States have developed or considered two types of direct access to e-evidence:

1) **Extended** access, i.e. use of a device of a suspect or witness seized as part of an investigation (e.g. with a search and seizure warrant) to access the data accessible from the device (which can include the cloud). Most Member States allow their public authorities to carry out this type of direct access.
2) **Remote** access to data with lawfully obtained credentials, i.e. a search from an authority's computer, usually not disclosed to the target until later. Only a few Member States allow their authorities to perform remote searches, although the number is increasing. Remote searches are often relevant in the context of investigations on the dark web, where there are no legitimate service providers whose cooperation could be obtained.

Although the use of extended or remote access as an investigative measure can be strictly domestic in nature, a cross-border situation is likely, e.g. where the infrastructure used for the data processing or the provider are in another country. The expert consultation process found that Member States have adopted different approaches to balancing the need for effective investigations of crime and possible extraterritoriality:

- when the storage location is **unknown**, (i.e. when there is **loss of location** and it is not possible to determine whether access to data would have a cross-border component), several Member States assume that the direct access takes place in a purely **domestic** context and permit securing the data, e.g. by copying it[58]; other Member States take the opposite approach and assume that the data is elsewhere and that access may have an **effect in another country** (although the data might in fact be domestically available)[59]. They will use an MLA request if able to identify the correct country.
- when the storage location abroad is **known**, a few Member States allow their authorities to access the data stored remotely **regardless** of the place of storage[60]; several Member States access the data and **contact or notify** the authorities of the

[58] In response to the September 2016 questionnaire, at least 4 Member States indicated that law enforcement and judicial authorities can access electronic evidence directly if it is unclear or even impossible to establish where the information is located (BE, ES, PT and FR).

[59] In response to the questionnaire, 8 Member States indicated that their authorities cannot themselves access electronic evidence when it is unclear what the location of the information is or when it is impossible to establish the location of the information (HU, SE, HR, CY, EL, LV, FI and SI) and 11 Member States clarified that this depends on specific circumstances (AT, EE, RO, SK, NL, CZ, DE, DK, UK, IT and LT).

[60] E.g. DK.

other country before deciding on how to proceed with the data[61]; and other Member States do not access the data directly and use formal or direct cooperation channels[62].

- Member States also have different approaches to **conditions and safeguards**. While **all** require judicial authorisation, conditions vary and can include a limit to cases of specific, e.g. serious forms of crime, reasonable grounds to assume that traces of a criminal act may be found on the device. These conditions also extend to the actions permitted: while all Member States permitting direct access allow for copying of the evidence, in some countries data may not be removed or only in exceptional cases.

While this diversity may reflect different legal cultures, it becomes an issue when a Member State allows its authorities to access data in a way that is perceived by another State as affecting its sovereignty/territoriality. Moreover, the level of rights of the persons whose data is accessed also varies considerably. In general, these different approaches to direct access in different countries may hamper investigations and prosecutions.

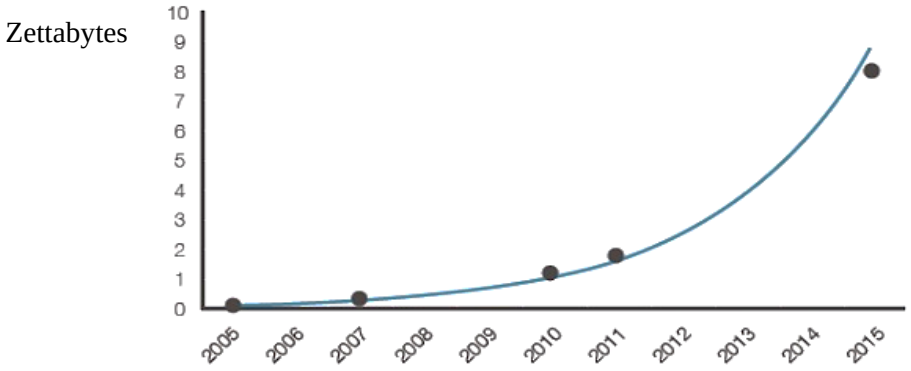
### 2.3. How will the problem evolve?

The main factors that will determine the evolution of the problem are the exponential growth of electronic data, the increasing need to access e-evidence across borders and changing systems for accessing data that would require updates to legislation.

1) The exponential growth of electronic data.

The digital age has brought exponential growth of electronic data:

*Figure 4: estimated worldwide data storage in zettabytes (trillions of gigabytes)*




Source: OECD

[61] E.g. BE, FR, NL.
[62] E.g. CZ, RO, DE.

This exponential nature not only brings exponential possibilities for economic and social development but also for crime, in two ways:

- Directly: all things being equal, cybercrime will continue to generate important economic benefits for criminals, justifying the amount of research and development hours required to produce malware, the main tool to carry out cybercrime (**every day**, more than 300,000 **new** malware samples are detected)[63]. The data related to cybercrime becomes electronic evidence that public authorities would need to access.
- Indirectly: by 2020 it is expected that up to **50 billion** new devices (cars, homes, medical devices, buildings, mobile phones, dishwashers, toys…) could be connected to the Internet[64]. This "Internet of Things" will generate massive amounts of information, which will translate into electronic evidence in the crimes that involve these devices and their users.

2) The increasing need to access e-evidence across borders.

As more and more countries join the technology revolution and more people around the world get connected to the Internet, the need to access e-evidence across borders will increase. Globalisation also implies **globalisation of criminal evidence.** Furthermore, the Internet does not only provide training materials to commit cybercrime or other crimes but also the necessary tools to commit crimes through the **crime-as-a-service** model[65]. More people connected unfortunately also means more potential criminals that could take advantage of those training materials and tools, likely at a **low risk**, as the challenges to cross-border access to e-evidence would remain untackled.

3) Changing systems for access that require updates to legislation (see Annex 12).

WHOIS data that was formerly publicly available is increasingly moving into systems that prevent unauthorised access by granting logins to legitimate users only, for individual look-ups in the context of criminal investigations. While authorities are considered as legitimate users and therefore would be granted access to the systems, this is only part of the picture. From an authority's perspective, any action needs to have a basis in law, and many national laws, including those of EU Member States, do not provide for one. In the absence of a specific legal basis, the database lookup might have to be replaced by a request or production order for each lookup.

In the **absence of EU intervention**, the problem drivers are likely to evolve as follows:

---

63 As reported by Kaspersky Labs, 2014.

64 The Internet of Things: How the Next Evolution of the Internet Is Changing Everything, Dave Evans, Cisco, 2011.

65 Crime-as-a-service is a business model that allows for the provision of cybercrime capabilities or ready to use cybercrime tools to other individuals or criminal groups.

1. Too much time would still be required to access e-evidence across borders under the judicial cooperation procedures, reducing the effectiveness of investigations and prosecutions.

   The exponential growth in electronic data will likely cause the number of request to continue increasing. If no action is taken to preserve the ability of authorities to perform WHOIS look-ups, these lookups may have to take the form of individualised requests that need to be reviewed individually. Given that such a lookup is often the first step in an investigation, a conservative estimate would put the number in the tens of thousands per week across the EU. In the absence of a legal basis permitting direct lookups, this procedure would significantly slow down investigative measures: the number of resources to deal with the requests throughout the process is not likely to increase accordingly (e.g. in MLAT requests to the US, public officials from requesting authorities, US Department of Justice officials, US judges and court officials, FBI agents, service providers' staff). This would likely result in even longer response times to MLAT (and EIO) requests. At the same time, data minimisation requirements force service providers to delete data more quickly, increasing the number of cases where data will no longer be available when the request reaches the service provider.

   The 2016 Review Report of the EU-US MLA Agreement concluded that there was no need to revise the Agreement, but included recommendations to make the Agreement work better in practice, including on electronic evidence. These include recommendations to seek direct cooperation from US service providers and consider other means to reduce the pressure of the volume of MLA requests to the U.S. for e-evidence, and to train and build capacity for public authorities, including on emergency procedures. The Commission has been encouraging Member States to implement the recommendations contained therein, and is helping to set up training (which is one of the practical measures proposed here), but practitioners and Member States agree that these recommendations are not sufficient to address the issues linked to the access to electronic evidence. Similarly as for the EIO, this is based on the consideration that without a fundamental change of the process, MLA procedures will never be as fast as direct cooperation channels. Emergency procedures are reserved for exceptional situations (involving imminent risk of serious injury or death, including in terrorism cases), while electronic evidence is required in a large proportion of all investigations.

2. Inefficiencies in public-private cooperation between service providers and public authorities would continue hampering effective investigations and prosecutions. As the response times for MLA (and EIO) requests would continue growing, public authorities would increasingly try to reach out directly to service providers, while these would be receiving more and more formal requests simultaneously. Without a clear framework for

direct cooperation between service providers and foreign public authorities it is likely that investigations and prosecutions involving e-evidence would become more and more challenging.

3. Shortcomings in defining jurisdiction would continue hindering effective cross-border investigation and prosecution. In the absence of EU intervention, the use by criminals of encryption, anonymisation tools, virtual currencies, the Darknet and other future technologies, or simply the use by service providers of technologies to manage the data that prevent its precise localisation, would continue making it difficult for public authorities to establish the appropriate jurisdiction. This may lead to the adoption by Member States of national legislation on direct cooperation with service providers, on direct access to e-evidence, or on other options such as data localisation, which would lead to a fragmented legal framework that could likely hamper effective cross-border cooperation in investigations and prosecutions.

The evolution of the problem in the absence of EU intervention will be further analysed when describing the baseline option.

## 3. WHY SHOULD THE EU ACT?

### 3.1. Legal basis

The legal bases for EU action are Articles 82(1), 82(2), 53 and 62 of the Treaty on the Functioning of the European Union (TFEU):

- Article 82(1) specifies that **judicial cooperation in criminal matters** shall be based on the principle of **mutual recognition.**
  This legal basis would cover possible legislation on direct cooperation with service providers (see options C and D), in which the authority in the issuing Member State would directly address an entity (the service provider) in the executing State and even impose obligations on it. This would introduce a new dimension in mutual recognition, beyond the traditional judicial cooperation in the Union, so far based on procedures involving two judicial authorities, one in the issuing State and another in the executing State.
- Article 82(2) would cover possible legislation on **direct access** (see option D), which would notably establish minimum safeguards and conditions when it comes to cross-border access to data that will protect the rights of subjects whose data is accessed.
- Articles 53 and 62 would provide for the adoption of measures for the coordination of the provisions laid down by law, regulation or administrative action in Member States concerning **establishment and provision of services**. Specifically, an obligation to

appoint a **legal representative** for the Union would contribute in particular to the elimination of obstacles to the freedom to provide services.

### 3.2. Subsidiarity: necessity of EU action

A satisfactory improvement of cross-border access to electronic evidence in criminal investigations cannot be sufficiently achieved by Member States acting alone or in an uncoordinated way. In the absence of EU action, Member States would have to update their national laws to respond to current and emerging challenges with the likely consequence of further fragmentation and/or conflicts of law, which would likely hamper cross-border cooperation in criminal investigations and prosecutions. Such individual action would also fail to provide a unified system for direct cooperation with service providers, leaving them to deal with more than 20 different legal systems instead of one harmonised approach.

Both the Member States and the European Parliament have recognised that these challenges require action beyond the national level. The June 2016 Council Conclusions gave a strong mandate to the Commission, and the October 2017 European Parliament Resolution also called for the Commission to put forward legislative proposals. This makes sense in view of the negative consequences of unilateral actions by Member States: if each Member State were to continue or start its own individual approach, then this would further increase the diversity of approaches and lead to possible conflicts related to the different conditions and safeguards for access.

For the access to e-evidence through online databases such as WHOIS, Member States have recently highlighted its importance in November 2017 Council Conclusions, where they cited "the importance of ensuring a coordinated EU position to efficiently shape the European and global internet governance decisions within the multi-stakeholder community, such as ensuring swiftly accessible and accurate WHOIS databases of IP-addresses and domain names, so that law enforcement capabilities and public interests are safeguarded"[66]. Given that the cross-border aspect cannot be sufficiently addressed by unilateral measures, access to the WHOIS database requires EU action because it also concerns cross-border access to non-public data. Such access creates international legal issues that are difficult to deal with by national legislation, which can by its nature only address national issues. Therefore the EU is well-placed to provide a harmonised solution, even if the ideal solution for any such problem would be at the global level, which is currently unrealistic to achieve and will likely remain so for a while.

---

[66] Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - Council conclusions (20 November 2017), ST- 14435/17.

EU action is needed on direct access because the systems adapted by various Member States are not coherent and risk creating conflict among Member States: while some impose few limitations on access to data stored abroad, others demand that law enforcement be able to prove that the data is stored in country out of respect for other countries' sovereignty. This impasse cannot easily be bridged at national level but only through coordinated action to define the conditions under which access may be granted.

As described in section 2.3., the current challenges to access e-evidence across borders are likely to keep increasing due to the exponential growth of electronic data, the increasing need to access e-evidence across borders and changing systems for accessing data that would require updates to legislation, as the world becomes more and more interconnected online. EU action to address these increasing challenges is not only necessary but also keenly expected by stakeholders, as repeatedly conveyed during the consultations, and at political level.

### 3.3. Subsidiarity: added value of EU action

Given the cross-border nature of the problem, the diversity of legal approaches, the number of policy areas concerned by the matter (security, criminal law, fundamental rights including data protection, economic issues) and the large range of stakeholders, the EU seems the most appropriate level to address the identified problems. As previously described, the crimes in which electronic evidence exists frequently involve situations where the victim, the perpetrator, the infrastructure in which the e-evidence is stored and the service provider running the infrastructure are all under different national legal frameworks, within the EU and beyond. As a result, it can be very time consuming and challenging for single countries to effectively access e-evidence across borders without common minimum rules.

The creation of EU cooperation mechanisms in criminal matters also reflects the value of action at EU level in this area. These mechanisms include legislation, such as the EIO Directive and institutions such as Eurojust. The added value of these initiatives in helping Member States access e-evidence across borders was acknowledged multiple times during the stakeholder consultations.

Another important added value of EU action is to facilitate cooperation with non-EU countries, in particular with the US, given that the need to access e-evidence internationally frequently goes beyond EU borders. This cooperation can also be better achieved at EU level than through bilateral agreements of individual Member States.

The objectives of the initiative can also be tackled at international level through instruments such as the Budapest Convention, where negotiations on a second additional protocol addressing e-evidence issues are taking place at the moment. A new set of rules at international level would be an essential but not sufficient element in addressing the issues

identified; it would not in itself address the problems identified as effectively as it might in combination with an EU instrument. This is due to expectation that the protocol, first, will not be as far-reaching as it is not based on the same level of mutual trust among the more diverse 50+ parties to the Convention and, secondly, will lack the enforcement mechanisms that EU law has, as it is an international Convention. EU action is therefore necessary.

## 4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

### 4.1. General objective

The general objective is to ensure effective investigation and prosecution of crimes in the EU by improving cross-border access to electronic evidence through enhanced judicial cooperation in criminal matters and an approximation of rules and procedures.

This general objective is in line with the legal basis contained in Article 82(1) TFEU on judicial cooperation in criminal matters, and in Article 82(2) TFEU, which empowers the EU to establish minimum rules concerning mutual admissibility of evidence and the rights of individuals in criminal proceedings to the extent necessary to facilitate mutual recognition of judgements and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension.

The general objective addresses the general problem of some crimes not being able to be effectively investigated and prosecuted in the EU because of challenges in cross-border access to electronic evidence.

### 4.2. Specific objectives

There are 3 specific objectives that address the problem drivers identified in section 2.2.:

*Table 5: problem drivers, specific objectives and general objective*

| Problem drivers | Specific objectives | General objective |
|---|---|---|
| 1. It takes **too long** to access e-evidence across borders under existing **judicial cooperation** procedures, rendering investigations and prosecutions less effective<br><br>2. Inefficiencies in **public-private cooperation** between service providers and public authorities hamper effective investigations and prosecutions<br><br>3. Shortcomings in defining **jurisdiction** can hinder effective cross-border investigation and prosecution | 1. **Reduce delays** in cross-border access to electronic evidence<br><br>2. **Ensure** cross-border **access** to electronic evidence where it is **currently missing**<br><br>3. Improve **legal certainty, protection of fundamental rights, transparency and accountability** | Ensure effective investigation and prosecution of crimes in the EU by **improving cross-border access to electronic evidence** through **enhanced judicial cooperation** in criminal matters and an **approximation** of rules and procedures |

## 5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

The following process was applied to determine the **policy options**:

1) **mapping** of possible policy **measures:**
    a. The mapping covered the full spectrum of possible EU intervention: no action, non-legislative action and legislative action.
    b. Given that the issue at hand is basically a **regulatory failure**, it was important to lay out the full range of regulatory tools to determine the most proportionate EU response.
    c. The mapping stage included a first filter to **identify** the policy measures to **discard** at an **early stage** (section 5.3.).
    d. The outcome of the mapping stage was a set of policy measures retained for further elaboration and analysis.
2) **description** of policy **measures** retained in the mapping stage (section 5.2.);
3) **analysis** of the policy **measures** retained in the mapping stage (Annex 4):
    a. This stage included a second filter to **identify** the policy measures to **discard** (i.e. the European Production Request and Order, the European Production Request and the recommendation on conditions and safeguards for cross-border online searches).

b. It includes a qualitative analysis using the same assessment criteria as those used to analyse the options. The policy measures **retained** are therefore those that provide the alternatives that are most feasible (legally, technically and politically), coherent with other EU instruments, effective, relevant and proportional to tackle the problem and its drivers analysed in section 2.
c. The outcome of this stage was the final set of measures for the policy options;

4) **description** of policy **options**, formed by combining the retained measures into different groups:
   a. The formation of options follows a **cumulative logic**, with an increasing level of EU legislative action (section 5.4.).
   b. The cumulative logic was followed not only because the measures are in general not mutually exclusive and can be combined but also because they are **complementary** in a number of ways, presenting **synergies** that the combined options can benefit from.
5) **analysis** of policy **options**:
   a. The options are analysed in detail in sections 6 (impacts), 7 (comparison of options) and 8 (preferred option).

### 5.1. Scope of policy measures

The scope of the policy measures for this initiative is the following:

- **Data** (material scope):
  - **Types** of data[67]:

[67] This classification is convenient as there are legal definitions for each of these categories in different legal instruments:
- a definition of **subscriber data** appears in Article 18(3) of the Council of Europe Convention on Cybercrime (CETS No 185): "any data held by a service provider, relating to subscribers of its services other than meta-data or content data and by which can be established: i) the type of communication service used, the technical provisions taken thereto and the period of service, ii) b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement, iii) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement";
- a definition of **electronic communication metadata** is included in Article 4(3)(c) of the Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final: ""data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication";

- **Non-content** data:
  - **Subscriber data**, which allows the identification of a subscriber to a service. Examples: subscriber's name, address, telephone number.
  - **Metadata**, which relates to the provision of services and includes "electronic communication metadata", as defined in the ePrivacy proposal[68]. Examples: data relative to the connection, traffic or location of the communication.
  - **Access logs,** which record the time and date an individual has accessed a service, and the IP address from which the service was accessed;
  - **Transaction logs,** which identify products or services an individual has obtained from a provider or a third party (e.g. purchase of cloud storage space)**.**
- **Content** data. Examples: text, voice, videos, images, and sound stored in in a digital format, other than subscriber or metadata.

The type of data may imply different treatment by existing rules and different procedures to access it. Each of the above categories may contain **personal data**, and are thus covered by the safeguards under the EU data protection acquis, but the intensity of the impact on **fundamental rights** varies between them, in particular between subscriber data on the one hand and metadata and content data on the other. Appropriate safeguards need to be provided in accordance with the level of **sensitivity**. The sensitivity of the data can also depend on the volume requested; large volumes of specific types of metadata can allow for the profiling of individuals, especially with respect to location, and hence require more safeguards as compared to smaller amounts or different kinds of metadata[69].

The above categories are all relevant for different purposes. Leaving any of them outside the scope would greatly diminish the effectiveness of the initiative.

---

- a definition of **electronic communication content** appears in Article 4(3)(b) of the proposal for a Regulation on Privacy and Electronic Communications above: "the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound".

[68] See previous footnote.

[69] See in that regard Judgement of the Court of Justice of 8 April 2014, Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12) (Joined Cases C-293/12 and C-594/12), in particular paragraphs 26 and 27.
See also the case Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others (Joined Cases C-203/15 and C-698/15), in particular para. 98 and 99.

- **Stored vs intercept**:
  - All the data above refers to electronically **stored data** that already exists**.**
  - **Intercept data** (i.e. data from real-time interception of telecommunications) is **out of the scope** of this initiative as there are specific and significantly different rules that determine access to that data (see measures discarded at an early stage, section 5.3.).
- **Concrete criminal offence vs mass surveillance**:
  - This initiative concerns cross-border access to e-evidence in the framework of criminal investigations or criminal proceedings for **concrete criminal offences**, which ensures the application of procedural guarantees.
  - Other situations not linked to a concrete investigation, such as **intelligence or mass surveillance**, are out of scope.
- **All data areas** are within the scope of the initiative.
- Types of **crimes**:
  - **All crimes** in the areas within the scope of the initiative are covered. The initiative is **not limited to serious crimes**, as the problem of cross-border access to e-evidence in criminal investigations is relevant for all crimes.[70]

- **Providers** of the following services (personal scope):
  - **electronic communications** services as defined in the proposal for a Directive establishing the European Electronic Communications Code[71]. The revised definition of electronic communications services covers both traditional telecommunication services (example: voice telephony, SMS, internet access service) as well as new internet-based services enabling inter-personal communications such as voice over IP, instant messaging and web-based email services (Over-the-Top communications services, 'OTTs'). These OTTs are in general not subject to the current EU electronic communications framework (i.e.

[70] See options discarded at an early stage, section 5.3. The current procedures to obtain e-evidence through for judicial cooperation, MLA and EIO, are not limited to certain types of crime. An EIO can be issued "in proceedings brought by administrative authorities in respect to acts which are punishable under the national law of the issuing State by virtue of being infringements of the rule of law", without being considered as criminal offences, as long as "the decision may give rise to proceedings before a court having jurisdiction in criminal matters". On the other hand, the EIO also allows the executing authority to refuse the execution of an EIO where "the use of the investigative measure indicated in the EIO is restricted under the law of the executing State to a list or category of offences or to offences punishable by a certain threshold, which does not include the offence covered by the EIO" (see Art. 11 para. 1 lit. (h), Directive 2014/41).

[71] Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), COM(2016)590.

Directive 2002/21/EC[72]), including the current ePrivacy Directive, which in general applies only to traditional telecommunication services. In line with the expansion of the EU electronic communications and ePrivacy framework, OTTs should be covered by this initiative as well (e.g. Gmail, WhatsApp);

- **information society** services as defined in the Directive 98/34/EC[73] that store data at the individual request of a recipient of a service; this includes a variety of known services providers such as social networks (e.g. Facebook and Twitter)**,** **cloud** services (e.g. Microsoft, Dropbox or Amazon Web Services), online marketplaces (e.g. eBay or Amazon marketplace) or other **hosting** service providers (e.g. Bluehost).
- **internet infrastructure** services such as IP address providers and domain name registries and registrars and associated privacy and proxy services (e.g. GoDaddy).

Service providers include both **data controllers and data processors**, as defined in Article 4(7) and 4(8) respectively of the General Data Protection Regulation.

- **SMEs:**
  - SMEs are also among the service providers covered. For effectiveness reasons, no general exemption for SMEs from the scope is proposed (see Annex 13).
- **Geography**:
  - All situations described in table 2 and figure 1, except the one in which countries A, B and C are outside of the EU (or A=B=C, in which case it is a national issue).
  - In particular, the initiative covers data **regardless of where it is stored**.
  - The initiative takes into account situations where the requesting public authority is from a non-EU country only with regard to **reciprocity** considerations.

## 5.2. Description of policy measures

The following sections summarise the description of the policy measures. More detailed descriptions are available in Annex 7.

### 5.2.1. Non-legislative action

Measure 1: practical measures to enhance judicial cooperation

[72] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[73] "Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

This measure would address problem driver 1 by making procedures for judicial cooperation more efficient, and specific objectives 1 and 2.

*a) Judicial cooperation with the US (MLA)*

The expert consultation process identified the following practical measures to enhance judicial cooperation between **public authorities in the EU and the US**, on the basis of the existing mutual legal assistance procedures:

1) **Organise regular technical dialogues with the US Department of Justice** to continue to improve the process, speed and success rate of MLA requests.
2) **Facilitate regular contacts between the EU Delegation to the US, the Commission and liaison magistrates** of Member States in the US to discuss MLA process issues.
3) **Provide opportunities for the exchange of best practice and further training** for EU practitioners on applicable rules in the US relate to the MLA procedure. The Commission has made available **EUR 500 000** under the Partnership Instrument[74] for this.

*b) Judicial cooperation within the EU (EIO)*

This measure proposes to facilitate the implementation of the EIO Directive through a set of measures that could improve the speed of judicial cooperation requests within the EU:

1) An **electronic user-friendly version** of the forms in the annexes of the EIO Directive.
2) A **secure online platform** for electronic exchanges of EIO/MLA requests and replies between EU competent authorities (including on e-evidence) to allow for swift and secure exchanges of requests between competent authorities of different Member States.

Measure 2: practical measures to enhance direct cooperation

This measure would address problem driver 2 by making procedures for public-private cooperation more efficient. It would address the specific objectives 1 and 2.

1) Creation of **single points of contact (SPOC)**, both on the public authorities' side and on the service providers' side:

[74] The Commission launched a call for proposals with a budget of EUR 1million total for improving cooperation both between judicial authorities of EU Member States and the US and between EU authorities and US-based service providers on 4 May 2017 under the Partnership Instrument Annual Action Programme 2016 Phase II - International Digital Cooperation - Component D – Cross Border Access to Electronic Evidence (EuropeAid/155907/DH/ACT/Multi). More information is available here.

- On the **public authorities' side** in the Member States, it could significantly improve the direct cooperation between those authorities and service providers by e.g. ensuring the quality of outgoing requests and building relationships of confidence with providers, as they know their counterpart.
- On the **service provider's side,** the creation of a single point of entry could also improve the direct cooperation between those authorities and service providers, by, e.g., helping to clarify the provider's policies.

2) **Streamline procedures** on both the public authorities' and the service providers' side:
   - On the **public authorities' side,** the **standardisation and reduction of forms** used by law enforcement and judicial authorities could facilitate the creation of requests by law enforcement and increase the confidence of service providers when it comes to the identification of authorities and proper forms used.
   - On the **service providers' side,** significant improvements could be made through **streamlining service providers' policies** to reduce the heterogeneity of approaches, notably regarding procedures and conditions for granting access to the requested data.
3) **Provide opportunities for the exchange of best practice and training** of public authorities in the EU on cooperation with US-based providers.
   - All stakeholders indicated that additional **training for law enforcement and judicial authorities** could support the functioning of direct cooperation between those authorities and service providers. The Commission has made available **EUR 500 000** under the Partnership Instrument[75] for improving direct cooperation.
   - Several stakeholders suggested the **establishment of an online information and support portal** at EU level to provide support to investigations, including information on applicable rules and procedures. It could leverage the work of existing initiatives such as Europol's **SIRIUS platform** to facilitate online investigations, including the direct cooperation between authorities and service providers[76].

#### 5.2.2. Legislative action

*International agreements*

The EU could seek to conclude international agreements coherent with EU-internal solutions to provide a basis for closer international cooperation with safeguards comparable to those of the EU-internal solution with regard to individuals' rights, including judicial redress. These agreements could cover judicial cooperation, direct cooperation and/or direct access.

---

75 *Ibid.*

76 This interactive platform would allow law enforcement authorities to collect publicly available information, to identify the relevant service providers for additional information, and to find the appropriate channel for making the request. More information is available here.

The objectives of these measures on improving cross-border access to electronic evidence through international agreements are:

- to ensure international comity;
- to ensure appropriate conditions and safeguards; and
- to institute mutually compatible approaches and reduce conflicts of law.

*Box 4: what is **international comity** and why does it matter?*

International comity is the practice of showing courtesy among nations. It refers to the disposition to perform some official act out of goodwill and tradition rather than obligation or law. In other words, it is the acceptance or adoption of decisions or laws by a court of another jurisdiction, either foreign or domestic, based on public policy rather than legal mandate.

In the area of cross-border access to e-evidence, international comity may be challenged when different countries use different connecting factors or direct access. For example, country A may perceive an action by country B as having a cross-border dimension affecting its territorial interests while country B regards the situation as purely domestic in nature; both countries will thus also disagree on the need to use domestic or cross-border channels to obtain the evidence concerned[77].

These measures consider the negotiation of two types of international agreements: multilateral and bilateral.

Measure 3: multilateral international agreements

This measure would seek to address problem drivers 1 and 3 by reducing the need for judicial cooperation and clarifying jurisdiction for investigative measures. It would also address problem driver 2 insofar as a multilateral agreement would include provisions on direct cooperation with service providers. All specific objectives would be addressed.

[77] See e.g.: U.S. Court of Appeals for the Second Circuit, Microsoft v. United States, No. 14-2985 (2d Cir. 2016) of 14 July 2016. The case is under review by the U.S. Supreme Court and a decision is expected by July 2018. See Annex 9 (Box 1) in this document for more details;
see also the Skype vs Belgium case (e.g. Stibbe, Skype Luxembourg condemned in Belgium for refusing to set up wiretap, 24 February 2017): Belgian authorities considered the request for data as a domestic request when the provider located in Luxembourg considered the request as a foreign request (in accordance with the current Luxemburgish legal framework).

Multilateral international agreements ideally create a common framework across a wide number of countries affected by the same challenge. In the field of cyber-enabled crime, the 2001 Council of Europe Convention on Cybercrime (the Budapest Convention) is the main multilateral framework[78].

The parties to the Budapest Convention recently decided to negotiate an additional protocol to the Convention by September 2019[79]. The scope may expand the existing framework allowing for **direct cooperation** with service providers in other jurisdictions (possibly including subscriber information, preservation requests, and emergency requests), as well as create a **clear framework and safeguards** for cross-border access to information.

The interest for the EU to follow closely the negotiation of this Additional Protocol is threefold:

1) Some non-EU countries which are also Parties to the Budapest Convention (e.g. the US) are very important in improving cross-border access to e-evidence.
2) While the scope is unlikely to extend to content data, it may include elements that are already covered by existing acquis at EU level, including on Mutual Legal Assistance or in relation to the European Investigation Order.
3) It may help address some of the **reciprocity** issues that a possible EU legislative initiative could generate (see option C, in particular Box 5).

The negotiations are closely linked with a possible EU proposal on e-evidence: if a proposal is made, consistency will have to be ensured, and there will also be a clear competency for the EU and obligation for the Member States to defend a common position. Whereas these negotiations will proceed regardless of EU action, the EU has the option to take a more or less active role in them. The main added value of an EU mandate to take an active role in these negotiations would be to ensure coherence and complementarity with a possible EU proposal on cross-border access to e-evidence.

Measure 4: bilateral international agreements

This measure would seek to address problem drivers 1 to 3 by reducing the need for judicial cooperation, regulating direct cooperation and clarifying jurisdiction for investigative measures. It would address all specific objectives.

[78] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace (JOIN(2013) 1 final of 7.2.2013).

[79] (DRAFT) Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, T-CY (2017)3, version 1 June 2017.

The EU could aim to conclude bilateral agreements to provide for production request/orders and direct access on a reciprocal base, possibly including rules for the enforcement of production orders. As the large majority of requests are sent to the US, an agreement with the US would have priority.

The US and the UK have been exploring the conclusion of a bilateral agreement to permit reciprocal direct requests to service providers for access to content data, subject to specific conditions and safeguards. This agreement requires a number of legislative changes, which are pending in the US.
The EU could aim to conclude a similar agreement with the US to allow direct requests to service providers for content data that currently cannot be disclosed by US service providers under the voluntary cooperation regime. Such an agreement would fall within the scope of application of, and would thus have to comply with, the EU-US Umbrella Agreement[80].

Beyond the US, further bilateral cooperation with countries member of European Economic Area and with other countries such as Canada could also be contemplated.

*Legislation on direct cooperation*

| |
|---|
| The following measures would seek to address problem drivers 1, 2 and 3 by creating a clear framework and thus reducing inefficiencies in direct cooperation and the need for judicial cooperation, and clarifying jurisdiction for investigative measures. |

These measures focus on addressing through a new legislative instrument problem drivers 2 (section 2.2.2.) and 3 (section 2.2.3.), which concern direct cooperation with service providers (i.e. situations in which the service provider has access to the data sought). It would indirectly also address problem driver 1 (section 2.2.1.), as an improved channel for direct cooperation would take pressure off the MLAT and EIO channels, saving them for those requests that require judicial cooperation mechanisms.

The new legislation in these measures would tackle the specific issues described in sections 2.2.2. (e.g. improving transparency, reliability, accountability and admissibility of evidence) and the issues concerning domestic production orders described in 2.2.3. (e.g. ensuring legal certainty, reducing conflicts of law, fragmentation and complexity, and protecting fundamental rights through procedural safeguards). It would indirectly also help reduce the

[80] The EU-US data protection "Umbrella Agreement" puts in place a comprehensive high-level data protection framework for EU-US law enforcement cooperation. More information is available here.

time required for judicial cooperation procedures, an issue described in section 2.2.1., by creating a new channel for requests.

For data access **with individual review by the service provider**, there are basically two ways in which legislation on direct cooperation with service providers can go:

- **Production requests** are **non-mandatory** instructions made by a public authority in a Member State directly to a service provider to disclose data under its control, without the involvement of the public authorities of the country where the service provider is based. The service provider can **voluntarily** provide the requested information. If the request is not complied with, there is no possibility of ensuring **execution**.
  As described in section 2, this is the type of direct cooperation that takes place with service providers headquartered in the US, albeit without a specific legal basis in most Member States.
- **Production orders**, in contrast, are **mandatory** instructions made by a public authority in a Member State directly to a service provider to disclose data under its control, without the involvement of the public authorities of the country where the service provider is based, and within a set **deadline**. Service providers can be obliged to execute them on the territory of the Member State in which they are issued and, depending on the approach chosen, also on the territory of the Member State in which they are served on the relevant service provider.

In addition, the **type of data** (i.e. whether **content or non-content**) is a key factor to take into account when defining possible legislative options for direct cooperation.

The combination of the two sets of key factors above (i.e. whether the instruction is voluntary/mandatory and whether for content/non content data) generates the following legislative measures for direct cooperation with service providers:

*Table 6: legislative measures for direct cooperation with service providers*

| Sub-option | Content | Non content |
|---|---|---|
| European Production Order (EPO) | Order | Order |
| European Production Request (EPR) | Request | Request |
| European Production Request and Order (EPRO) | Request | Order |

All the measures above **share** the scope, definitions of types of e-evidence and the obligation for service providers to appoint a legal representative:

1) **Scope**:
   - All the measures in the above would share the same scope, which is the one defined in section 5.1 for this initiative, across its various dimensions:
   - Data (material scope):
     - Content and non-content, stored (not intercept), concerning concrete criminal offences (no mass surveillance), all crimes (not limited to serious ones) in all areas.
     - Data should be provided regardless of whether the service provider is able to decrypt the data or disclose it in encrypted form only.
   - Service providers (personal scope):
     - The service providers within the scope of this legislative acts would be those listed in section 5.1.
     - The scope needs to be comprehensive enough to create an effective tool, yet clear enough to allow providers to reliably assess whether they fall into the scope. A concrete list of type of service providers concerned provides clarity and legal certainty, and was therefore preferred to a "negative list" approach, including all service providers whose services might generate electronic evidence and excluding a limited number of service providers, or an open provision without any list.
   - Geography:
     - In line with the geographical scope described in section 5.1., these legislative measures would cover **data regardless of where it is stored**[81], as well as **service providers regardless of where they are based**, as long as they offer services on the EU market. "Offering services" on the EU market would be determined by a number of possible indicators, e.g., the availability of the service in an EU Member State language not widely spoken outside the EU or the possibility to pay for services in Euro.[82] The mere accessibility of the service from the EU would not be sufficient.[83]
     - Other connecting factors were not retained, in particular:

---

81 The Proposal for a Directive to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, COM(2017)142 final, follows a similar approach. It provides national competition authorities with the right to require information irrespective of where it is stored, provided that it is accessible to the addressee of the request for information (see in particular recitals 23 and 26, and Articles 6 and 8).

82 The Budapest Convention Committee recently adopted a guidance note on the use of domestic production orders for subscriber information against service providers with a business link to the country of the issuing authority (i.e. "offering its services in the territory of a Party" to the Convention): Convention Committee (T-CY) of the Council of Europe Budapest Convention on Cybercrime, Guidance Note #10 - Production orders for subscriber information (Article 18 Budapest Convention), 1 March 2017, T-CY (2015)16.

83 A similar approach is followed in EU competition, consumer protection and data protection laws.

- **Data storage** location:
  - if used as a connecting factor, it essentially leaves it up to the choice of service providers whether and where access to data should be granted and what rights apply;
  - it has little to no connection to the case at hand, or even to the user;
  - in certain situations, it might also create difficulties for authorities if they cannot discern the data storage location when making a request and are not in a position to verify providers' statements about where data is stored;
  - it would also leave compliance with production orders to the discretion of service providers or their users, who could easily choose to store their data out of reach of the instrument, despite strong links to the investigating jurisdiction.
- **Service providers' location**:
  - regardless of their market presence in the EU, service providers could choose to avoid establishing themselves in the EU;
  - service providers established outside of the EU may face a conflict of obligations between EU and national law of the country where they are established, in particular in the case of production orders. The different sub-options would include a procedure to resolve these conflicts of law (see below under "Sanctioning mechanism").

2) **Definitions of types of e-evidence**:

- All the measures in this section would share the **legal definitions** of the types of electronic evidence. Harmonizing these definitions would provide for a common understanding and legal certainty for all the stakeholders concerned by the legislation.
- These definitions would take into account **existing definitions**, such as those in the Council of Europe Convention on Cybercrime and the proposal for an ePrivacy Regulation (see section 1 for more details on these legislative acts).
- The differentiation between different categories of e-evidence would allow to take into account **different requirements** by law or jurisprudence for one or more categories.
- To ensure that the definitions are not only **future-proof** (i.e. not affected by technological developments) but also **precise, clear and comprehensive**, stakeholders suggested the creation of a **technical library**, built in cooperation with Member States and service providers. This library would contain information about and examples of the different types of e-evidence as defined by the legislation and would, e.g. provide clarity where the interpretation varies at present.

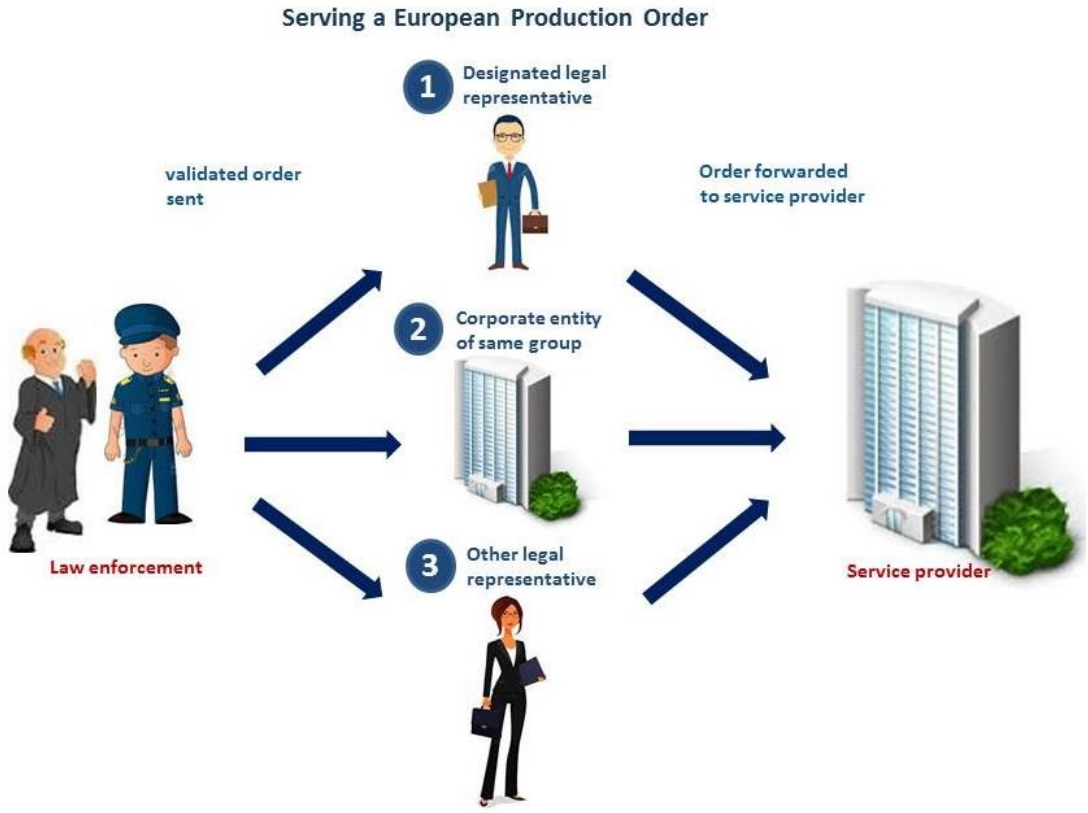
3) The **legal representative**:

- **Overview:**
  - The expert process identified the importance of **obliging** service providers to designate at least one legal representative (a natural or legal person) in at least one of the participating Member States to facilitate direct cooperation between the public authorities of the requesting Member State and the service provider.
  - The condition that triggers the designation of a legal representative would be the **provision of services** on the EU market (see "Geography" section above). The legal representative model could draw, e.g., on the same approach as the legal representative for data protection purposes.
  - Exemptions or mitigation criteria could be considered, similarly to those contained in Art. 27 GDPR. An exemption could e.g. apply when the processing of personal data of EU data subjects is occasional. For effectiveness reasons, no general exemption for SMEs from the obligation to designate a legal representative is proposed (see Annex 13).
- **Purpose:**
  - The purpose of the legal representative would be to facilitate direct cooperation by turning the process of serving production orders/requests to service providers established outside the Union into an **EU-internal process**.
  - The same legal framework would apply to all service providers with a significant presence in the EU, whether or not they have their seat in the EU.
- **Function**:
  - The legal representative would have to be able and authorised by the service provider to **receive, process and comply** with production orders and/or production requests. It would be left up to the service provider's internal organisation how compliance would be accomplished, which would not necessarily have to be performed by the legal representative (see below).
  - In the case of production orders, the legal representative would also be the person through which legal obligations could be **enforced** by means of administrative **sanctions** imposed on the service provider.
  - In case of service providers established **outside of the EU**, the legal representative would enable the production orders and/or requests to be served and, in the case of production orders, enforced in the EU. Member States have asked to also have a legal representative designated in case of service providers established **in the EU**, in order to have a clear addressee for production orders and/or production requests.
  - The legal representative would be an intermediary with no need for specific **control or access to data**. The designation of such a representative would not

affect the responsibility or liability of the service provider (i.e. the service provider would remain the one liable and responsible). Like the legal representative under Article 27 of the GDPR[84], it is therefore a **procedural tool** to facilitate direct cooperation and enforcement.

- **Choice** of legal representative:
  - In principle, providers should be **free** to designate as legal representative one or several entities in the EU and may choose to accumulate separate functions in one and the same person (e.g. GDPR or ePrivacy representatives[85]).
  - One representative could be shared among a number of service providers. This could be particularly relevant to avoid excessive burden for SME's.

The following flowchart illustrates the possible alternatives for serving an EPO:




[84] Article 27 of the GDPR obliges certain data controllers to designate a representative in order to facilitate the cooperation with the data protection authorities and allow for the enforcement of the EU data protection rules to the extent they apply to the foreign data controller, according to the GDPR's scope of application.

[85] For the ePrivacy representatives, see Art. 3 of the ePrivacy proposal, Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final.

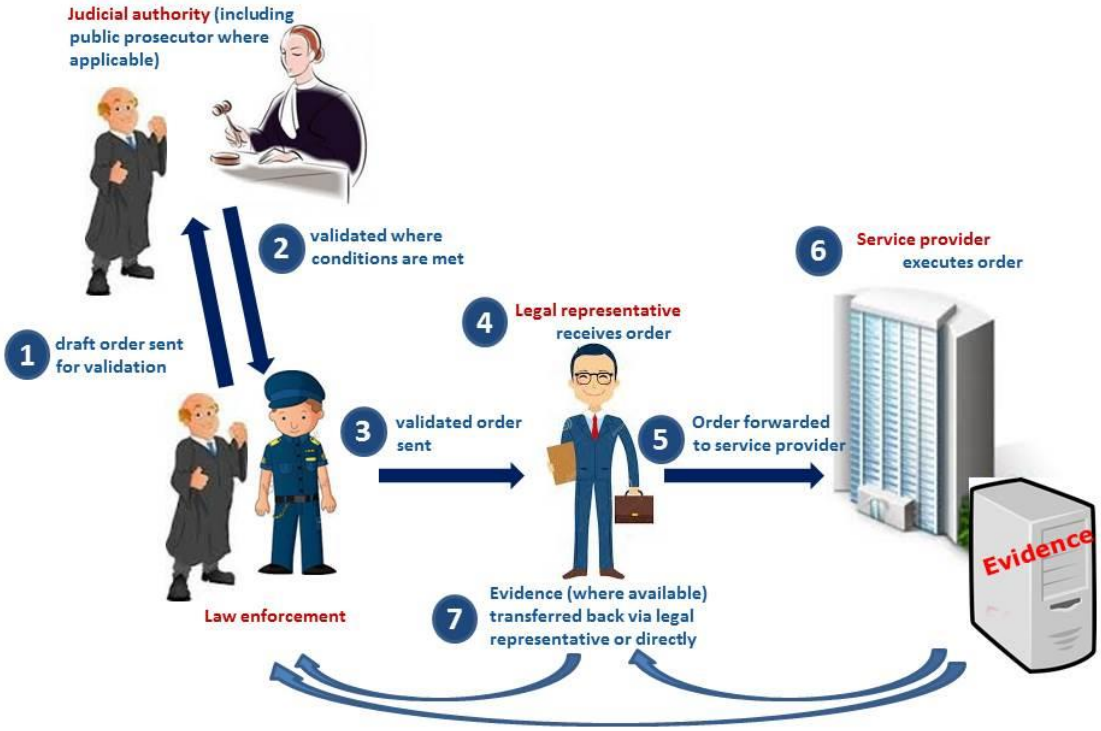
The following sections describe the **specificities** of each of the related measures.

Measure 5: European Production Order

1) **Overview:**

- This measure proposes a cross-border **European Production Order**, an official demand issued or validated by a judicial authority of a Member State for the disclosure of information stored in digital form that could serve as evidence in the framework of criminal investigations or criminal proceedings.
- The European Production Order could be directly addressed to a service provider outside of the Member State where it is issued, irrespective of where the service provider is based (i.e. whether in another Member State or outside of the EU) and of where the data is stored. The European Production Order would be **binding**, i.e. the service provider has an **obligation** to cooperate when so required by the competent authority and could face fines in case of non-compliance.
- It would also provide for deadlines to respond. These deadlines could be two-fold: a deadline for normal cases, which would give the service provider a reasonable period to reply to orders, and a deadline for urgent cases, which could be accompanied by a lighter procedure. This would also address the issue of timing of obtaining e-evidence, which is a crucial aim of the initiative.

Simplified illustration of procedure:



2) **Sanctioning mechanism:**

- Authorising authorities to compel a service provider to disclose e-evidence in cross-border cases and obliging service providers to respond can only be **effective** in practice if there is a possibility for **execution** of such orders in case of non-compliance. While compliance with a legal obligation might still be expected from a number of companies, without a possibility for sanctioning in case of non-compliance, the European Production Order would in practice resemble a production request, as the obligatory nature would be merely theoretical. The added value would thus be limited.
- Currently, not all Member States have a legal framework in place for imposing **financial sanctions** against non-compliant service providers in their national laws.
- As a minimum, the legal proposal under this measure should therefore impose an obligation on Member States to set up **effective, proportionate and dissuasive sanctions**. A **harmonised** framework for financial administrative sanctions could also be envisaged to avoid discrepancies between Member States for similar situations.[86]
- In order to maximise the efficiency of the new instrument, the proposal could include provisions on the **imposition and execution of sanctions**:
    - **Within the EU**, the imposition and execution of sanctions could be entrusted to the Member State where the service provider is based, based on **mutual recognition** mechanisms.
    - **With non-EU countries**, should a financial sanction be imposed against a company based outside the EU, the legal representative would also be served with the decision imposing sanctions on the service provider. Such a financial sanction could be executed in a non-EU country only through **applicable international agreements**, as the legal proposal could not oblige the authorities of non-EU countries to execute the sanction.
- **Conflicts of law**:
    - The need to avoid creating new conflicts of laws was raised repeatedly by service providers, civil society and some Member States during the consultations. This is particularly relevant when the service provider is based in a non-EU country (e.g. the US).
    - **Conflicting obligations** for service providers could arise from the national law of non-EU countries, as this EU instrument would cover data stored outside of the EU and service providers established outside of the EU or subject to the law of a non-EU country. In particular, service providers could be caught

[86] As an example, the maximum penalty currently set out in Hungarian law is EUR 5 000.

between the obligation to comply with a European Production Order and the law of the non-EU country applicable to the data or the service provider, which may prohibit or restrict/condition such disclosure of data to foreign authorities. An example is the **US Electronic Communication and Privacy Act**, which prevents companies under US jurisdiction from sharing content data directly with foreign law enforcement.

- This issue could be addressed by means of a **dedicated procedure** for reviewing such conflicting obligations in the issuing Member State. In case of a conflict of obligations arising from the law of a non-EU country, the service provider could invoke that conflict on the basis of a reasoned refusal to comply. In case of disagreement between the issuing authority and the service provider, a court could be asked to review the case. The court and the issuing authority could also engage in consultations with the other country's authorities. The judge could eventually **either uphold the order** (if he finds there is no conflict of law) **or lift the order** (if he finds there is a conflict of law) and **order preservation of the data** while awaiting mutual legal assistance from the authorities of the other country.
- As an auxiliary measure to the European Production Order, the legal proposal would include the possibility to execute an **order to preserve the data**, which would be sent by the competent authority directly to the service provider[87].
- Measures to **prevent abuse** of such a "conflict of law clause" would need to be considered. For example, the criteria mentioned above should be limited to relevant types of legislation such as criminal procedural law and data protection law.
- Such a clause would, in addition to protecting service providers from conflicts of law, also address potential issues of **extra-territoriality**, i.e. the intrusion on the sovereignty of the non-EU country, and of **reciprocity**, i.e. legitimisation of similar production orders by non-EU countries with respect to data held in the EU or providers headquartered in the EU. Reciprocity issues would be particularly problematic if they involved countries which do not have fundamental rights safeguards in place that can be considered comparable to those in the EU, including in the field of data protection[88], and if the relevant legislation in those countries did not provide for comparable conditions and

[87] Currently, requests for expeditious preservation of data can be sent from the authority in one country to the authority of another country under Art. 29 of the Cybercrime Convention, and followed up by an EIO/MLA request. Preservation requests can also be sent under Art. 32 of the EIO Directive.

[88] See e.g. Chapter V of the General Data Protection Regulation (EU) 2016/679 (GDPR) with regard to transfer of personal data by service providers to a non-EU country.

safeguards as those that should be included in any European Production Order proposal. The conflict of laws clause could contribute to mitigating the intrusiveness of the measure, from both an international law and privacy point of view, and would ensure international comity. Because the conflicting laws of non-EU countries would be taken into account, the Union and Member States could claim that these countries should do the same when requesting electronic evidence from an EU service provider, e.g. when there is a conflict with the EU data protection regime. This would mitigate the risk that our data protection acquis is undermined by non-EU countries.

3) **Safeguards:**

The European Production Order would be accompanied by comprehensive safeguards, which could include the following:

a) **Procedural rights** of accused and suspected persons:
   - The suspect would be protected by the EU acquis on the rights of suspected and accused persons in criminal proceedings and the full respect for due process.
   - In particular, Directive 2012/13/EU on the right to information in criminal proceedings [89] grants the suspected or accused person access to all material evidence in the possession of the competent authorities at minimum, in order to safeguard the fairness of the proceedings and to allow for preparation of the defence.

b) Intervention of a **judicial authority:**
   - Every European Production Order would have to be issued or validated by a judicial authority.
   - In most Member States, law enforcement authorities can order service providers in their own jurisdiction to disclose **subscriber data**. The cross-border European Production Orders would have to be validated by a judicial authority. This creates an additional safeguard and also matches the approach taken in the European Investigation Order.
   - Furthermore, the legal basis of this initiative, Article 82 TFEU, refers to "**judicial** cooperation in criminal matters (…) based on the principle of mutual recognition of **judgments** and **judicial** decisions."
   - The intervention of a judicial authority would generate greater **mutual trust** and contribute to greater reassurance for the service providers receiving the order. It would also ensure that the **proportionality and legality** of the measure have been

[89] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings.

checked and that the order does not infringe **fundamental rights** such as the lawyer-client privilege or the right to media freedom.

c) Charter of Fundamental Rights including the principles of **necessity and proportionality:**
   - The judicial authority would have to ensure the respect of the Charter of Fundamental Rights including by taking into account the principles of **necessity and proportionality** in its decision to issue or validate a production order, and specific aspects to consider could be enumerated. These should include that the data sought, including the data category, is necessary for and the measure is limited to what is necessary and proportionate to the purpose of the proceedings, also in view of the nature and gravity of the offence under investigation (petty crime versus more serious offences).

d) Principle of **"controller first":**
   - The production order should by preference be **addressed to the data controller**, i.e. the entity that determines the purposes and means of the processing of personal data (Art. 4(7) GDPR). This could be of relevance in particular when it comes to larger entities, such as corporations, that avail themselves of the services of service providers within scope of this instrument to provide their corporate IT infrastructure and/or services.
   - However, for cases where this is **not opportune**, e.g. because the controller itself is suspected of involvement in the case under investigation or of otherwise colluding with the target of the investigation, authorities should be able to address a service provider able to provide the data in question.

e) **User notification:**
   - By **public authorities**, in line with national criminal procedural laws which provide for notification and with Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities (the "Police Directive")[90], which establishes:
     - a right for the data subject to be **personally informed** by the competent authority about the data processing in specific cases, in particular where the personal data are collected without the knowledge of the data subject (Article 12 et seq);

[90] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

- that this right to be informed may be **delayed, restricted or omitted** to "avoid obstructing official (…) investigations [and] prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties" (Article 13(3)(a) and (b)); and
- that such a restriction requires a **legislative measure** and can only be imposed to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned (Article 13(3)).

o By the **service provider**:
- An **immediate notification** to the user could jeopardise the investigation and is therefore not provided in the criminal procedural laws of most Member States.
- For the same reason, the legal framework would include a provision that gives the issuing authority the right to **prohibit or delay** the notification to the user by the service provider for such cases.
- The affected person would have to **be informed** as soon as the risk of obstructing the investigation no longer exists. At the latest, this occurs when taking open measures against the affected person, e.g. bringing charges in court or arresting the person.
- If a decision is taken not to prosecute the suspect or the investigation is closed or abandoned, user notification should in principle be done at this point, to avoid circumventing the obligation to notify[91].

f) **Legal remedies:**

o For the **target of the investigation**:
- The remedies in Member States against national production orders vary substantially: from no legal review (except for the accused person during his trial) to the right for every affected person to seek judicial review.
- It is essential that the suspect whose data is requested in the framework of criminal investigations or proceedings can have access to an effective legal remedy in the issuing country. The legislation should therefore set out, as a minimum, the possibility for the accused to challenge during the trial the

[91] Even if the initial case is closed, there might be cases where the data is relevant for another case, and informing the data subject might jeopardise this other case (example: the evidence is needed against another person or the evidence is essential for a whole new case). In these situations, where the use of data collected in one case for another case is lawful, law enforcement should have the possibility to delay the user notification further.

legality of an European Production Order as well as the admissibility (or the weight in the proceedings) of the evidence obtained by such means.
    - Remedies for situations without trial should also be considered.
    - Remedies should in any case not have suspensive effect, like the EIO. The proposal could refer to legal remedies provided by national law available in similar domestic cases as provided in Article 14 of the EIO Directive.
- For **service providers:**
    - Service providers may be also be affected by the investigative measure.
    - The situation in Member States varies from no legal review, as the service provider is regarded as a third party unaffected by the investigation, to the possibility to challenge the order, which only exists in few Member States.
    - Given the ambitious approach of the European Production Order, service providers should have the possibility to react in particular cases, including:
        - requesting legal review if the European Production Order has not been issued or validated by a judicial authority;
        - requesting legal review if the metadata requested is erroneously qualified as subscriber data;
        - asking for clarifications if the request is unclear
        - claiming any remedies set out in national law of the issuing state for a domestic case.
    - In cases of non-compliance, the (separate) decision to impose a fine should be subject to legal remedies, as it directly affects the service provider.
    - In all these cases, legal remedies should be brought before the courts of the issuing State. Even though it would be easier for the service provider to bring an action to its domestic courts, it should be the courts of the issuing State who should review decisions of issuing authorities in accordance with the applicable law of the issuing State. The courts in the State of the service provider would not be well-placed to apply the criminal procedural law of another Member State to control the authorities of this other Member State. This could lead to conflicts between Member States, and would create a risk of diverging decisions.
- For **third persons** (e.g. **victims, witnesses**):
    - In addition to suspects and service providers, third persons (e.g. **victims or witnesses**, whose data is requested) may be affected by the investigative measure.

- A legal remedy could also be considered for third persons whose data was sought and who do not have the opportunity to challenge the legality of the order in a subsequent trial against the accused person[92].
- The right of any data subject to lodge a complaint with a supervisory authority under the data protection rules must also be respected[93].

g) **Privileges and immunities**:

- Judicial cooperation in criminal matters in the Union has so far relied on mutual recognition involving two authorities, i.e. a judicial decision taken in one Member State is recognised and executed in another Member State. Since the entry into force of the EIO this also applies to the access to evidence.
- The EIO contains a limited set of grounds for non-recognition or non-execution (Article 11). These include cases in which there is an immunity or privilege under the law of the country receiving the EIO (e.g. for certain professions such as medical and legal) and absence of dual criminality. Because of their importance,[94] the European Production Order should include the possibility for some of these grounds for non-recognition or non-execution to be taken into account in the issuing State during the trial, e.g. if raised by the accused person[95]. In addition, the issuing judicial authority should be obliged to carefully assess a number of criteria before issuing the order, e.g. that persons benefiting from immunities are not affected by the order.
- Subscriber data should be left outside the scope of these grounds for non-recognition or non-execution due to its lesser sensitivity, and because this is regularly the first step in identifying a person. This is already recognised to some extent in the EIO, where double criminality cannot be invoked as ground for refusal for subscriber data (Articles 11(2) and 10(2)(e)).

Measure 5*: European Production Request (EPR)

1) **Overview:**

- The European Production Request would provide, through the production request, a harmonised legal basis across Member States to recognise the legality of the current practices of direct cooperation and to further enable such cooperation between Member State by removing existing hurdles and prohibitions. It would provide judicial

92 Similar considerations apply when no trial takes place against the suspect.

93 In coherence with Articles 52 and 53 of Directive 2016/680 ("Police Directive"), for any data subject whose data was in his/her opinion unlawfully processed.

94 The importance to ensure application of the lawyer-client privilege has been raised by the CCBE during the public consultation.

95 A systematic notification of the receiving State was considered as too burdensome, see discarded options.

authorities with the competence to make non-binding requests for cross-border access to electronic evidence to service providers located in another Member State or outside of the EU, and for these service providers to reply to such requests, without passing through local law enforcement or judicial authorities. The main added value of production requests is that they would provide legal certainty for a process that is currently not clearly regulated in Member States' laws. This is advantageous from a fundamental rights perspective and adds clarity to a non-transparent system

1) **Sanctioning mechanism :**
   - There would be no sanctioning mechanism for the European Production Request could not be executed in the country of the service provider.
2) **Safeguards:**

   The same safeguards as for the European Production Order would apply, with the exception of:
   - the immunities and privileges which should not apply to a non-executable instrument;
   - the conflicts of laws clause, as no specific review procedure is required if service providers can simply choose not to comply, forcing authorities to recur to traditional tools for formal judicial cooperation.

In addition, the fact that the request cannot be executed creates a further safeguard in the form of the possibility for the service provider not to comply in case of doubt as to the legitimacy of the request. While this assessment should not be outsourced to the service provider, this could be a de facto consequence of the non-enforceable nature of the European Production Request.

<u>Measure 5**: European Production Request and Order (EPRO)</u>

2) **Overview:**
   - This measure would take the form of a production **request** for **content** data. The European Production Request and Order would provide judicial authorities with the competence to make **non-binding** requests for cross-border access to **content** data to service providers located in another Member State or outside of the EU, and for these service providers to reply to such requests, without necessarily passing through local law enforcement or judicial authorities.
   - For **non-content** data, it would be the same as the European Production Order. The European Production Request and Order would introduce a harmonised legal basis across Member States for issuing **production orders** for **non-content** data, taking one step further the current practices of direct cooperation for non-content data on a voluntary basis.

3) **Sanctioning mechanism:**
   - For **content** data, there would be no sanctioning mechanism., as the measure would in essence be voluntary.
   - For **non-content** data, the sanctioning mechanism would be idem the European Production Order.
4) **Safeguards:**
   - For **content** data, the same safeguards as for the European Production Order would apply, with the exception of :
     - the immunities and privileges which should not apply to a non-executable instrument;
     - the conflicts of laws clause, as no specific review procedure is required if service providers can simply choose not to comply, forcing authorities to recur to traditional tools for formal judicial cooperation.

     In addition, the fact that the request cannot be executed creates a further safeguard in the form of the possibility for the service provider not to comply in case of doubt as to the legitimacy of the request. While this assessment should not be outsourced to the service provider, this could be a de facto consequence of the non-executable nature of the production request.
   - For **non-content** data, the safeguards would be idem the European Production Order.

Measure 6: access to data without individualised review (WHOIS)

| |
|---|
| This measure would seek to address problem driver 1 by reducing the need for judicial cooperation. It would address specific objective 1. |

For data that service providers **make available for access by authorities through a system of databases** without individual review by the service provider (e.g. the WHOIS systems), legislation could provide for a legal basis to perform searches in the system, in line with the rules of the system, national frameworks and EU law, including data protection rules. The main added value of a legal base to access online databases such as WHOIS would be to maintain the same possibility for access once the information is no longer publicly available. Currently, WHOIS information is extensively used by law enforcement, in particular as the starting point for investigations. Once the information is no longer publicly available, those possibilities would disappear and access would be subject to the more strictly conditions required for more intrusive searches, which however were not conceived for this situation. This would in turn frustrate the start of investigations.

**1) Scope**:

- Data (material scope):
  - Subscriber information, stored (not intercept), concerning concrete criminal offences (no mass surveillance), all crimes (not limited to serious ones).
- Geography:
  - In line with the geographical scope described in section 5.1., this legislative measure would cover **data regardless of where it is stored**[96]. **Data storage** location is not a feasible connecting factor for a worldwide federated data access system underpinning a global resource such as the domain name or IP address systems.

**2) Safeguards:**

Safeguards could include the following:

a) **Procedural rights** of accused and suspected persons:
   - The suspect whose data is accessed would be protected by the EU acquis on the rights of suspected and accused persons in criminal proceedings and the full respect for due process.
   - In particular, Directive 2012/13/EU on the right to information in criminal proceedings [97] grants the suspected or accused person access to all material evidence in the possession of the competent authorities at minimum, in order to safeguard the fairness of the proceedings and to allow for preparation of the defence.

b) Principles of **necessity and proportionality:**
   - The authority would take into account the principles of **necessity and proportionality** in its decision to access records in the database system, and specific aspects to consider could be enumerated.

c) **User notification:**
   - **Authorities** would have to notify users in line with national criminal procedural laws which provide for notification and with the Police Directive[98].

---

96 The Proposal for a Directive to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, COM(2017)142 final, follows a similar approach. It provides national competition authorities with the right to require information irrespective of where it is stored, provided that it is accessible to the addressee of the request for information (see in particular recitals 23 and 26, and Articles 6 and 8).

97 Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings.

98 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

d) **Legal remedies:**
   - For the **target of the investigation**:
     - The suspect whose data is requested in the framework of criminal investigations or proceedings must have access to an effective legal remedy in the issuing country. The legislation should therefore set out, as a minimum, the possibility for the accused to challenge during the trial the legality of the database lookup as well as the admissibility (or the weight in the proceedings) of the evidence obtained by such means.
     - A remedy in case of no trial should also be considered.
     - The proposal could refer to the legal remedies provided by national law available in similar domestic cases.

There would be no added administrative burden compared to today, besides implementation, as the measure proposes to maintain the same procedures as today, i.e. not requiring individual judicial review. This measure could usefully be combined with either the European Production Order, the European Production Request and Order or the European Production Request. While this measure and the latter three address different aspects of direct cooperation, they are complementary and do not overlap, as they cover different cooperation mechanisms.

*Legislation on direct access*

Measure 7: legislation on harmonised safeguards for direct access

| |
|---|
| This measure focuses on addressing through a new legislative instrument problem driver 3 (section 2.2.3.), specifically the part that concerns direct access to e-evidence across borders from an information system within the jurisdiction. It would address specific objective 3, and to a more limited extent, 1 and 2. |

This measure focuses on addressing through a new legislative instrument problem driver 3 (section 2.2.3.), specifically the part that concerns direct access to e-evidence across borders from an information system within the jurisdiction.

In particular, the new legislation under this measure would allow public authorities to access data directly when it is not certain that the data is stored in the same Member State, and also set minimum standards. It would define a set of **conditions** for the issuing of a judicial order permitting direct access, as well as a number of **safeguards**. The aim would be to establish common principles for accessing data that may be stored outside of the issuing Member State, thereby reducing **fragmentation** and increasing **mutual trust** among Member States .

1) **Scope:**
   - Types of investigative actions covered:
     - Direct access with the **agreement of the data subject**: e.g. if a victim or witness gives access to his or her mailbox to allow the authorities to view a relevant exchange with a suspect.
     - **Extended** search in the context of an **ongoing search** under national law: e.g. when a person is searched on the basis of a warrant that extends to the search of any digital device the person is carrying.
     - **Remote** search based on **lawfully obtained user credentials:** e.g. when authorities use login information obtained during a house search to access a dark web forum the suspect was active on.
   - Material scope:
     - Content and non-content, stored (not intercept), concerning concrete criminal offences (no mass surveillance).
   - Geography:
     - In line with the geographical scope described in section 2.1.1., these legislative measure would cover **data regardless of where it is stored**, for the reasons described in sections 2 and 5, and to ensure that it encompasses the wide range of existing solutions in place in the Member States.
2) **Conditions:**
   - The conditions should be enumerated in an exhaustive list, following the examples of the European Arrest Warrant[99] or the Europol Regulation[100].
   - The legislation would cover **at least serious crimes** and would leave it up to the Member States to cover also other types of crime, or cover all types of crimes.
     - Direct access to data always takes place in the framework of a national investigative measure (e.g. seize and search). National law frameworks impose different conditions on the use of these investigating measures, which may include **limitations** with regard to the **types of crime** that would be applicable for obtaining the data stored on the device or in a cloud, when it is allowed.
     - By establishing that Member States could introduce such measures **at least for serious crimes** without preventing them from going further, the proposal would allow Member States to adapt the provisions to their specific situation.
     - Serious forms of crime could be defined, like in mutual recognition instruments, through a list of crimes or through criteria established in the

[99] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ 190/1.

[100] Regulation 2016/794/EU of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), OJ L 135/53.

proposal (e.g. by referring to a minimum sanction of a crime), in a way that **avoids conflicts** with the national frameworks.
    - At the same time, imposing conditions and safeguards for serious crime only would open a path for Member States to apply less conditions and lower safeguards to direct access for lesser crimes. This might be inappropriate given the need to ensure proportionality of conditions and safeguards to the situation at hand, including the severity of the offence. Viewed from that perspective, it could be counterproductive to impose stricter conditions for more serious offences only.
- Specific conditions for direct access **with the agreement** of the data subject.
    - The data subject (the suspect or a third person) would have given his or her agreement to access his or her data stored in another territory, irrespective whether it is via the device of the data subject or via another computer system in the investigating State.
    - National law would have to provide an appropriate legal basis for the processing of personal data to comply with the Police Directive which requires a legal basis either in national or in European law, even when the data is processed with the agreement of the affected person.
    - A similar situation is already covered by the Budapest Convention[101], which provides for a search with the consent of the person who has the authority to disclose the data through a computer system in the territory of the investigating state.
- Specific conditions for an **extended** search in the context of an **ongoing search** under national law:
    - Direct access through a seized device would be covered if there is an **ongoing search** (and seizure) of an electronic storage medium located in the territory of the investigating State on the basis of national law **with the knowledge** of the affected person.
    - The data concerned has to be considered **necessary** for the investigation; furthermore, direct access to the data would have to be **required in order to avert the threat of losing the data**. This threat can be particularly acute in the context of an open search as the suspect becomes aware of the investigation and may seek to destroy evidence. However, if swift cooperation from a service provider can be expected, direct access should not be necessary.
- Specific conditions for a **remote** search based on **lawfully obtained user credentials**:

[101] See Article 32, Trans-border access to stored computer data with consent or where publicly available.

- Direct access to data stored remotely through an authority's device would be covered if the credentials to an online account have been lawfully obtained.
- The credentials can have been provided by a person other than the service provider, or found during the search of a premises or a device.
- The knowledge of the user would not be required.
- The data concerned again has to be considered **necessary** for the investigation; furthermore, direct access to the data would have to be **required in order to avert the threat of losing the data**. The same considerations set out immediately above also apply.

- The conditions applicable for the search of the data on the device itself already set out by the respective **national law** would be preserved.

3) **Safeguards:**
   - **Procedural rights** of accused and suspected persons (idem European Production Order, see above).
   - Intervention of a **judicial authority:**
     - Any of the forms of direct access covered by the legal act would have to be validated by a judicial authority.
     - The decision by the judicial authority to validate a form of direct access would take into account the respect of the Charter of Fundamental Rights including the principles of **necessity and proportionality**, taking into account that:
       - Access should be limited to what is **necessary and proportionate** to the purpose of the proceedings, also in view of the nature and gravity of the offence under investigation.
       - In addition, direct access to the data would have to be necessary in order to avert the **risk of losing the data**, or because of other exigent circumstances[102].
       - In case of remote access, the suspect is often unaware of the measure. As a result, the risk of deletion of evidence by the suspect is reduced. Therefore, remote access could be considered in situations where other forms of access (e.g. direct cooperation with service providers) are:
         - **not possible or cannot be considered as feasible**: e.g. the location of the provider is unknown, such as Telegram; or in case of use of the Dark net, where it is rarely possible to

[102] For example, the risk of losing the data is high when, in the context of an open search, the suspect becomes aware of the investigation and may seek to destroy evidence. In such a situation, judicial cooperation between public authorities or direct cooperation with service providers may not be fast enough.

determine the identity of the service provider because of the techniques used to conceal the origin of the information/data;

- could seriously **undermine the investigation**: e.g. in covert investigations to infiltrate paedophile networks. A remote search could be conducted in the course of the covert operation, and without compromising the covert investigation.

  - Access should be limited to securing the data by **copying** it.

- **User notification:**
  - Where direct access takes place without the knowledge of the user concerned, user notification needs to be ensured.
  - The relevant considerations set out above for the European Production Order for user notification by public authorities (i.e. in coherence with Directive 2016/680) would also apply.
- **Legal remedies:**
  - The possibility for judicial review in the issuing State in accordance with its national law should be ensured.
  - The relevant considerations set out above for the European Production Order for legal remedies (including for third persons such as victims or witnesses) would also apply.
- The safeguards applicable for the search of the data on the device in **national law** (including e.g. thresholds and privileges) would be preserved.
- A drawback lies in the fact that the measure could add to the existing **administrative burden** in Member States that already have direct access measures in place, as it may impose additional conditions and safeguards.
- These additional conditions and safeguards might result in **restricting direct access** to a narrower set of conditions as currently in place in those Member States that enable direct access. This is a result of an overall balancing act between the interest in effective investigation and prosecution of crimes and the fundamental rights of targets of those investigations, a balance that may have been determined in different ways at national level.

Measure 7*: recommendation on conditions and safeguards for cross-border online searches

| |
|---|
| This measure seeks to address problem driver 3 (section 2.2.3.), specifically the part that concerns direct access to e-evidence across borders from an information system within the jurisdiction. It would address specific objective 3, and to a more limited extent, 1 and 2. |

This measure seeks to address problem driver 3 (section 2.2.3.), specifically the part that concerns direct access for e-evidence across borders from an information system.

Although this measure does not involve legislation at EU level, it could entail legislation in Member States, hence its inclusion under legislative action. A recommendation would set out a non-binding set of minimum standards for cross-border direct access to e-evidence. These minimum standards could be adopted by Member States and made part of national laws governing direct access. The recommendation would define **conditions** for the issuing of a judicial order permitting direct access, as well as a number of **safeguards**. The aim would be to provide common principles for accessing data that may be stored outside of the issuing Member State, thereby reducing **fragmentation** and increasing **mutual trust** among Member States. Given the non-binding nature, the impact of the measure would largely depend on Member States' willingness to adopt the proposed conditions and safeguards.

1) **Scope:**
   The recommendation would have the same scope as Measure 7 with respect to types of investigative measures covered, material and geographic scope.
2) **Conditions:**
   - The conditions should be enumerated in an exhaustive list.
   - The recommendation would cover all types of crimes. Imposing conditions and safeguards for serious crime only would open a path for Member States to apply less conditions and lower safeguards to direct access for lesser crimes. This would be not logical and in fact inappropriate given the need to ensure proportionality of conditions and safeguards to the situation at hand, including the severity of the offence.
   - The specific conditions for the three types of direct access measures to be set out in the Recommendation would be the same as those outlined above under Measure 7.
3) **User notification:**
   - The Recommendation would suggest that, where direct access takes place without the knowledge of the user concerned, user notification needs to be ensured.
   - The relevant considerations set out above for the European Production Order for user notification by public authorities (i.e. in coherence with Directive 2016/680) would also apply *mutatis mutandis*, given that a Recommendation is a non-binding instrument.
4) **Legal remedies:**
   - The Recommendation would suggest that judicial review in the issuing State in accordance with its national law should be ensured.
   - The relevant considerations set out above for the European Production Order for legal remedies (including for third persons such as victims or witnesses) would also apply *mutatis mutandis*, given that a Recommendation is a non-binding instrument.

- The safeguards applicable for the search of the data on the device itself already set out by the respective **national law** (including e.g. thresholds and privileges) would remain unaffected by the Recommendation.

### 5.3. Measures discarded at an early stage

This section lists the policy measures discarded at an early stage. Please see Annex 8 for a complete analysis of the reasons why the measures were discarded.

1) Non legislative action.
   - Practical measures to enhance judicial cooperation among public authorities and direct cooperation between public authorities and service providers.
     - Within the EU:
       - Develop a **platform** to centralise the communication between service providers and public authorities across the EU.
       - Facilitate coordination of **service providers** to achieve **full harmonisation** of policies, standards and forms to provide access to e-evidence.
       - Leverage **ETSI (European Telecommunications Standards Institute) standards** for lawful interception in telecommunications to facilitate the interactions between public authorities and service providers across the EU.
     - Modify the **EIO form** contained in the annex to the EIO Directive to adapt it better to the needs of cross-border access to e-evidence.
     - With non-EU countries:
       - Develop a common online **form**[103] for MLAT requests to the US which could help public authorities in Member States to better comply with US requirements, in particular for probable cause in the requests for content.
2) Legislative action.
   - Legislative measures on **judicial and direct cooperation**: amendment of the **EIO Directive** to include provisions on e-evidence.
   - Legislative measures on **judicial cooperation**: **international agreements**.
     - Promote a new **United Nations convention** on cross-border access to e-evidence, which would replace the Council of Europe Convention on Cybercrime.
   - Legislative measures on **direct cooperation** with service providers.
     - Introduce mandatory **data localisation**, i.e. require service providers offering services in the EU to store their data in the EU.

[103] The President's Review Group on Intelligence and Communications Technologies already highlighted in 2013the possible convenience of creating an online submission form for MLATs to streamline the process, Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, December 12, 2013.

- Restrict the **scope** of the legislation to **data stored in the EU**.
- Introduce an **obligation** for service providers **to decrypt encrypted data** before giving access to public authorities to e-evidence.
- Limit the **scope** of application of the European Production Order to **certain crimes** (e.g. serious crimes).
- Use as a **connecting factor** to exercise jurisdiction:
  - the **accessibility of the service** (e.g. web site or app) from the EU;
  - the **pure corporate presence** in the EU of a service provider;
  - the **nationality of the suspect.** Some of the service providers currently use this criterion to decide whether to cooperate voluntary with foreign public authorities (e.g. a service provider only facilitates access to e-evidence to Italian law enforcement if it concerns Italian nationals).
  - any factor susceptible to be shaped by **internal company policies**.
- Use as a criterion to require service providers to designate a **legal representative** in the EU that the service has at least **1 million users** in the EU.
- Oblige service providers to nominate **a legal representative in every Member State** in which they are active or which they are targeting.
- Allow to address an European Production Order to **any corporate presence** of the service provider in the EU, without requiring service providers to nominate a legal representative in such cases.
- **Rely on non-EU countries** for service of orders to service providers established in those countries.
- Enter into an **agreement with the US** to allow service of documents directly in the US on US-based service providers.
- Use under the European Production Order a **notification system** to the receiving State (where the service provider is located) with the right to object within 96 hours.
- A production **request** for **non-content** and a production **order** for **content** data.

- Legislative measures on **direct access** to electronic evidence.
  - Set up an **EU legal basis** for direct access to electronic evidence.
  - Harmonise at EU level **search and seizure** measures.
  - Restrict the scope of the legislation to service providers with a given **connection to the EU**.
  - Restrict the scope of the legislation to data stored in the EU (i.e. **data storage** requirements).
  - Introduce **mandatory notification** to the **public authorities** of the country of habitual residence of the target of the measure by the public authorities of the Member State carrying out the measure.

- Introduce **mandatory notification** to the **public authorities** of the country where the data is stored.

### 5.4. Description of the policy options

The detailed analysis (see Annex 4) of the policy measures retained in the mapping stage discarded the following measures:

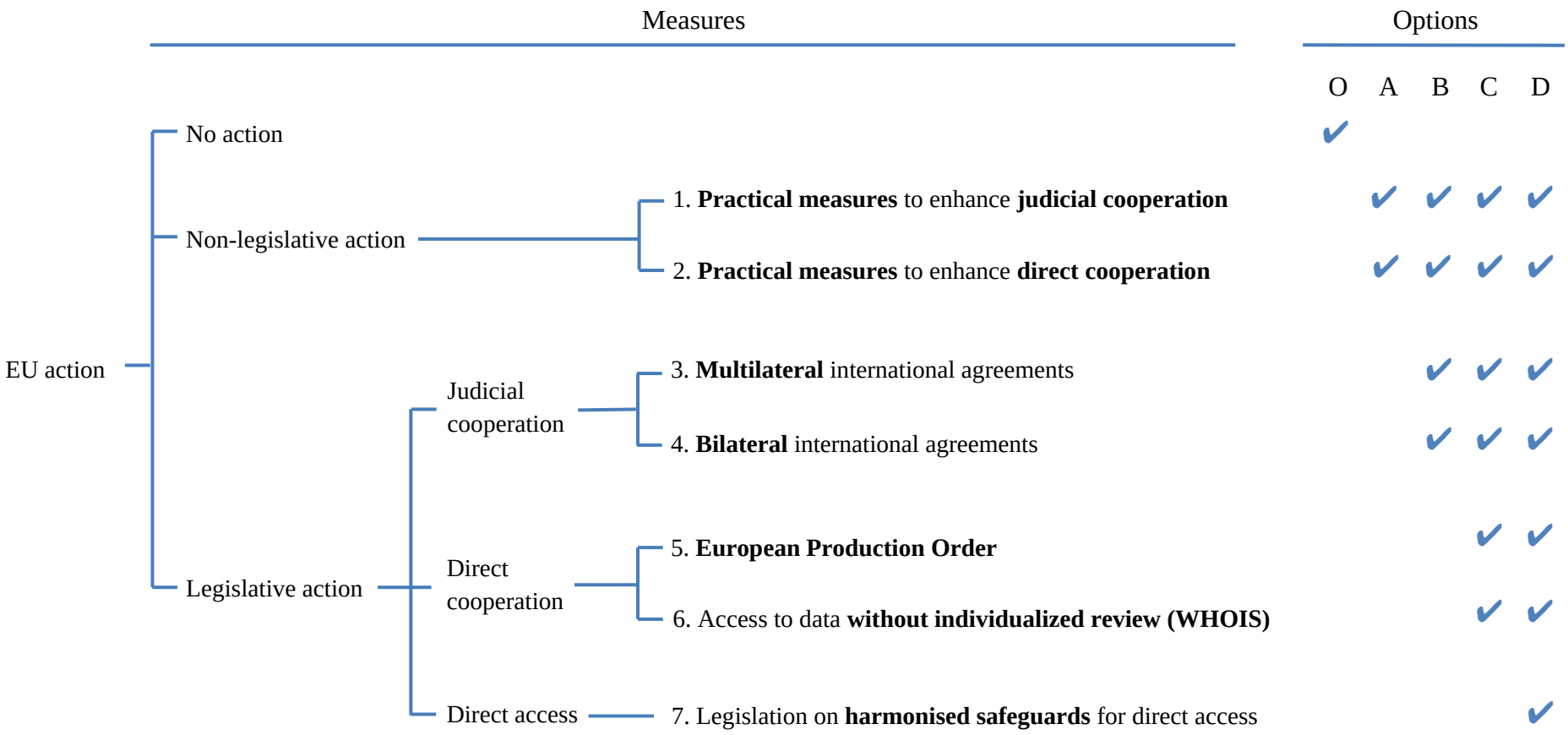
- in direct cooperation:
  - European Production Request (measure 5*);
  - European Production Request and Order (measure 5**);

  Both measures were discarded for being less effective without bringing any additional benefits compared to the European Production Order. See Annex 4 for further details.
- in direct access:
  - recommendation on conditions and safeguards for cross-border online searches in direct access (measure 7*).

    This measure was discarded because given its nonbinding nature, its effectiveness would likely be limited. Its main benefit would lie in further increasing fundamental rights protections; however, these possible benefits are outweighed by the lack of legal certainty and the added risk of fragmentation. See Annex 4 for further details.

The figure below provides an overview of the measures 1 to 7 retained to form the policy options A to D. It also includes the baseline (option O):

*Figure 5: mapping of policy measures and policy options*



### 5.4.1. Option O: baseline

This section summarises the baseline scenario. More information is available in Annex 9.

The baseline or **option O** is the scenario in which there is **no EU action**. This scenario has several dimensions:

1) **In general** terms, the problem drivers are likely to evolve as described in section 2.3. (How will the problem evolve), worsening the situation.
   - **Judicial cooperation** would likely take longer, given the exponential growth of electronic data and the increase in requests due to the loss of publicly available data, which is unlikely to be matched by a growth in resources to deal with the increased number of MLAT/EIO requests.
   - Without a clear framework for **direct cooperation** between service providers and public authorities:
     - the efficiency of this cooperation is, similarly, likely to decrease under the strain of the ever increasing number of requests. In addition, the sheer growth in volume of direct requests might create a disincentive for new or continued cooperation;
     - in the absence of a clear **legal basis** in national law, law enforcement may be unable to make requests for direct cooperation that are in compliance with Directive (EU) 2016/680 (the "Police Directive" or the **data protection** directive for law enforcement)[104] and in particular with Article 39, which sets specific conditions for such requests;
     - for data that is publicly available at present but will move into gated-access systems by May 2018 (WHOIS), when the new data protection framework comes into effect, availability to law enforcement will cease, absent a specific legal basis to address the data protection and criminal procedural law requirements.
   - Without a clear EU framework defining **jurisdiction** in cross-border access to e-evidence, Member States are likely to introduce different practices and legislative instruments at national level which would lead to **fragmentation** and hamper effective cross-border cooperation in investigations and prosecutions. This would also further exacerbate the challenges service providers already face in assessing many different legal systems and may adversely affect the willingness of service providers to continue to invest in cooperation in which they are not obliged to participate.
2) **Existing and incoming EU legislation** is not likely to effectively address the challenges in cross-border access to e-evidence, in the absence of specific EU action to address those challenges in each of the channels.

[104] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

3) **International agreements** between Member States and non-EU countries are likely to evolve in an uncoordinated way without EU action.
   - Council of Europe Convention on Cybercrime:
     - Negotiations on a new protocol will go ahead regardless of whether the EU acts. In the absence of EU action (i.e. active participation in the negotiations, ensuring coordination among Member States), the strength of a coordinated negotiating position would be lost, possibly with suboptimal consequences for Member States.
     - At the same time, the protocol by itself will most likely not address the problems identified as effectively as it might in combination with an EU instrument. Such a protocol, first, will not be as far-reaching as it is not based on the same level of mutual trust among the more diverse 50+ parties to the Convention and, secondly, will lack the enforcement mechanisms that EU law has, as it is an international Convention.
     - If the EU adopts its own legislative proposal on cross-border access to electronic evidence, the need for an active participation becomes even more evident as coherence between EU law and the Convention should be ensured. Otherwise Member States might be forced to choose between compliance with either the new protocol of the Convention or the new EU legal framework.
   - Bilateral agreements
     - Judicial cooperation between public authorities through the MLA process could also be influenced by the decision of the US Supreme Court on the **Microsoft Ireland case**, expected by July 2018.[105] The DOJ had previously sought access to content data from service providers in the US (also on behalf of requesting EU Member States) regardless of where it was stored. Microsoft challenged this practice in 2013 (see box below). The US Supreme Court could compel US service providers to produce e-evidence regardless of where it is stored (including evidence stored in the EU), or could limit US competence. This may further increase fragmentation.
     - In the absence of EU action, the current MLATs between the EU and non-EU countries would not be updated. In this scenario, Member States would likely be inclined to update or sign new bilateral agreements with non-EU countries, in particular with the US, to expand direct cooperation possibilities, leading to **fragmentation** that may hamper international cooperation in investigations and prosecutions. Member States themselves have expressed during the consultations the desire to avoid such a country-by-country approach if possible.
     - The recently **proposed legislation by the DOJ** may contribute to that fragmentation.
4) **Direct cooperation** between service providers and public authorities could evolve in a wide range of possible ways, none of which the EU would have the opportunity to

[105] See in Annex 9 the box on Microsoft case.

shape and contribute to in the absence of EU action, likely shaped by the outcome of a relevant case on access to electronic evidence stored abroad (the "Microsoft Ireland" case) and the DOJ proposal[106] to amend the US ECPA. However, these possible changes were not taken into account in detail for the purposes of the baseline because it is at present unclear if and how the US Congress will proceed on these issues, in particular because the US Supreme Court on 16 October 2017 accepted to hear the Microsoft Ireland case.

5) **Direct access** to electronic evidence could increase, as Member States could introduce new legislative and non-legislative initiatives on direct access, possibly increasing fragmentation and hampering cross-border cooperation.

In summary, the baseline scenario not only falls short in addressing the concerns expressed by stakeholders, but in the absence of EU action those concerns are likely to increase as the situation worsens across multiple dimensions.

#### 5.4.2. Option A: non-legislative action

This option groups all the non-legislative actions. It aims to address **problem drivers 1 and 2** by improving judicial cooperation, both with the US and in the EU, and direct cooperation channels, thereby reducing delays and ensuring access in situations where it is currently not possible.

#### 5.4.3. Option B: option A + international agreements

This option combines the non-legislative measures with international solutions. It aims to address **all problem drivers** by improving judicial cooperation and direct cooperation channels, thereby reducing delays and ensuring access in situations where it is currently not possible, and by reducing the need for judicial cooperation and clarifying jurisdiction for investigative measures.

#### 5.4.4. Option C: option B + direct cooperation legislation

This option, building on option B plus access to databases and a European Production Order, aims to address **all problem drivers**, proposing a package of solutions to improving cross-border access to electronic evidence in criminal matters. It aims to achieve all specific objectives.

Regarding the direct cooperation legislation, the European Production Order has been retained as preferred option, because of its increased effectiveness compared to the European Production Request and the European Production Request and Order.

This option builds on the fact that the implementation of non-legislative measure does not exclude legislative measures and vice versa. Furthermore, the options can complement each other, in particular since the practical measures:

---

[106] On 23 March 2018 the US Congress adopted the Clarifying Lawful Overseas Use of Data (CLOUD) Act, right before the adoption of the EU legislative proposals that this impact assessment accompanies. The CLOUD Act is available here.

- are not likely to address on their own all the current challenges, such as the **fragmentation** of legal frameworks in Member States, which was identified as a major challenge by service providers seeking to comply with requests based on different national laws, as previously described. Also, the practical measures cannot provide **legal certainty**, **transparency, accountability and fundamental rights safeguards** that the legal measures provide;
- **depend** on the **willingness** and commitment of other public authorities (including in non-EU countries like the US) and service providers to cooperate and implement them on a voluntary basis, which increases the unpredictability of their results. In other words, they lack the **enforcement mechanisms** and the **scope** that the **European Production Order** could provide (i.e. mandatory compliance with requests for **content and non-content data**); and
- could be combined with the European Production Order in specific ways. For example, the **single points of contact** for service providers described in measure 1 could be used also for the **legal representatives** of service providers targeting the EU market with their services or providing services in the EU market.

This option also builds on the complementarity of the legislative measures proposed under direct cooperation those concerning international agreements. For example:

- They are complementary in the **situations** in which they **apply**. For example, the judicial cooperation determined by the international agreements (e.g. MLA) would apply to Member States which would not opt in the European Production Order and to non-EU countries.
- A bilateral agreement (in particular with the US), could help reduce the **conflict of laws** that the European Production Order could cause, or at least ensure an efficient procedure to address situations of conflict of laws. It could also take cooperation with key partner countries to a higher level, building on the Council of Europe Convention on Cybercrime and taking it above the cooperation level which can be achieved through the Convention, which brings together a more heterogeneous group of countries.
- A multilateral agreement such as the additional protocol in the Council of Europe Convention on Cybercrime could address **reciprocity** issues arising from the legal measures for direct cooperation:
    - For example, with regard to the European Production Order, it could address the minimum conditions and safeguards applicable to similar production orders by a number of non-EU countries with respect to data held in the EU or by providers headquartered in the EU. Also, it could improve for those countries the effectiveness of the procedure to apply the conflict of laws clause in the European Production Order.

*Box 5: possible **reciprocity** issues arising from the legislative options*

Legislative measures that entail reaching out to data stored in another jurisdiction, such as the European Production Order or direct access, might trigger a reciprocal

response by non-EU countries in which they try to access data stored in the EU.

- In the case of the **European Production Order**, if the EU legislated to impose an obligation on intermediaries in non-EU countries to provide e-evidence to public authorities in the EU, this may incite non-EU countries to impose similar obligations on intermediaries subject to EU law, which in turn could place them under a conflict of law, in particular with the EU data protection rules. This situation is already contemplated in Article 48 of the GDPR. The negotiation of an Additional Protocol on the basis of proper EU coordination would increase the probability that the resulting instrument, setting the appropriate standards at international level, would provide the international standards required for the intermediaries in the EU to comply with their obligations under the GDPR and avoid conflicts of law.
- In the case of **direct access**, a wider interpretation of the concept of loss of location applied by non-EU countries "in reverse" may generate fundamental rights issues resulting from the access of non-EU countries to personal data of EU citizens, if the country does not ensure due process and legal safeguards in place that can be considered comparable to the EU standard, including in the field of data protection[107].

On the other hand, at a time when some non-EU countries have already adopted or might be tempted to adopt unilateral approaches for obtaining electronic evidence (e.g. data localisation obligations or a more expansive set of investigative measures), creating a framework for access to electronic evidence that builds on the robust protections already provided for under EU law and including specific safeguards could set **a positive example**. This could possible discourage some countries from following the above unilateral approaches or rely on reciprocal responses that deviate from EU standards.

This approach would also create a useful complement to the **EIO and to MLA procedures**. For investigations that concern both electronic and other types of evidence, authorities are free to choose to make two separate requests (which might be desirable if swift action is required to safeguard the electronic evidence) or to submit one joint request. Several investigative measures can be included in the same MLA or EIO request, provided that they are requested from the same Member State or non-EU country. Regarding electronic evidence, there will be few cases where the Member State of establishment of the service provider would also be asked to carry out other investigative measures, as the seat of the service provider is often the only link to the other Member State. In cases where there is indeed a stronger link to that other Member State, the issuing Member State could choose to only issue an EIO, combining all investigative measures sought from the non-EU country.

[107] See e.g. Chapter V of the General Data Protection Regulation (EU) 2016/679 (GDPR) with regard to transfer of personal data by service providers to a non-EU country.

### 5.4.5. Option D: option C + direct access legislation

This option aims to address **all problem drivers** across **all three channels**, proposing a holistic solution to improving cross-border access to electronic evidence in criminal matters. It aims to achieve all specific objectives.

This option builds on the complementarity of the legislative measures proposed under direct cooperation and legislation on direct access. For example:

- They have similar **scope:**
  - Material scope, as both cover content and non-content, stored (not intercept), concerning **concrete** investigations of criminal offences (no mass surveillance), in all areas, and excluding machine to machine data[108].
  - Geography, as both would cover data regardless of where it is stored.
- They have similar **safeguards**, i.e. concerning procedural rights, intervention of a judicial authority, user notification and legal remedies.
- They are complementary in the **situations** in which they **apply**:
  - **Direct access** would be applied in situations where there is no service provider, where cooperation with the service provider is not fast enough to avoid the risk of losing the data, not possible, or could undermine the investigation, as previously described.
  - **Direct cooperation** on the basis of the European Production Order would be applicable in the rest of the situations where direct cooperation with the service provider is possible.

This option would also build on the complementarity of the measures under international agreements and those under direct cooperation. For example:

- A multilateral agreement such as the additional protocol in the Council of Europe Convention on Cybercrime could address **reciprocity** issues arising from the legal measures for direct cooperation.
- The international agreement could address the fundamental rights issues that could result from the direct access of non-EU countries to personal data of EU residents without ensuring due process and legal safeguards comparable to EU standards.

## 6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

### 6.1. Qualitative assessment

The qualitative assessment of the options based on their social, economic and fundamental rights impacts[109] was done in two stages:

---

[108] The only difference is that option D would cover **at least** serious crimes, leaving to Member States whether to cover other types of crime, whereas option C would cover any type of crime by default.

[109] As none of the options are considered to have a major environmental impact, apart from a potential effect on the investigation and prosecution of environmental crime, and a small reduction in paper usage through digitalisation of processes through measure 2, the environmental impact will not be assessed.

1) Qualitative assessment of the policy measures (see Annex 4).
2) Qualitative assessment of the policy options (this section), based on the above assessment of the corresponding measures.

#### 6.1.1. Social impact

As the objective of the initiative is to ensure effective investigation and prosecution of crimes in the EU, the focus of the social impact assessment is on crime and security, in particular on public authorities' capacity to investigate and prosecute criminal activity. Any improvement of this capacity could also lead to improved deterrence for criminals, better protection of victims and improved security for EU citizens. According to Member States' input, cross-border access to e-evidence is relevant for more than half of all investigations, and many investigations come to a dead end because of failed access. Therefore, any improvement of cross-border access could have a positive impact on Member States' capacity to investigate and prosecute crime.

**Option O: baseline**

In the baseline scenario, authorities' capacity to investigate and prosecute crime will not improve, but is rather expected to be further reduced. This is due to the exponential growth of electronic data and the move away from publicly available data, requiring judicial cooperation procedures where formerly a direct lookup sufficed. In addition, lower or no roaming fees create incentives for criminals to use the cheapest providers in the EU for throwaway phones, regardless of Member State, expanding cross-border use. Together, these changes are likely to create a significant burden on the current system.

As previously described, judicial cooperation would probably take longer. Countries are unlikely to invest at the necessary level to deal with the increased number of MLAT/EIO requests, especially where they do not see a need for these procedures. This is particularly true for countries like the US which are taking steps to decrease reliance on judicial cooperation procedures when foreign authorities contact service providers established there. Such countries would not necessarily see a need to invest more in procedures that, from their perspective, are superfluous. They would only be motivated by an interest in serving the needs of partner countries.

Similarly, in the absence of a mandatory legal framework, direct cooperation between service providers and public authorities is likely to suffer under the strain of the ever-increasing number of requests. Feedback from the consultation process indicates the clear and growing limitations of the existing process (see Annex 2). Without an EU framework for cross-border access to e-evidence, and in view of the clear need expressed both at expert and ministerial level, Member States are likely to introduce different practices and legislative instruments at national level, which de facto cannot foster harmonisation and would lead to fragmentation. Uncoordinated solutions could also create conflicting obligations for service providers, and increase the administrative burden inherent in many different national solutions. This development is already taking place: for example, Italy has put forward new draft legislation to impose an obligation on service providers active there to nominate a legal representative in Italy. Italian authorities could thus serve domestic production orders on these companies, and have domestic enforcement tools at their disposal.

These likely developments, taken together, could create further obstacles to access e-evidence, resulting in an increased number of delays and unanswered requests. In addition, as companies within and beyond the EU start implementing stronger data protection rules, data minimisation and related rules should lead to swifter deletion of metadata in particular, in the absence of a specific legal basis for the retention. Inefficiencies and delays in data requests would lead to a growth in unanswered requests as the data would have been deleted already. This could result in less effective investigations and prosecutions, which in turn could lead to a decreased deterrent effect, less effective protection for victims and a lower overall perception of security.

**Option A: non-legislative action**

The practical measures to enhance judicial cooperation between public authorities in the EU and in the US, in particular the training of EU practitioners and the sharing of guidelines and best practices, would to some extent improve the quality of MLA requests submitted by EU authorities and would therefore both accelerate the treatment of these requests and improve their success rate.

The establishment of a platform for online exchange of e-evidence between EU competent authorities and the creation of an electronic form for EIO requests is expected to facilitate judicial cooperation between competent authorities of Member States, allowing them to secure and obtain e-evidence more quickly and effectively. Regarding direct cooperation with service providers, the foreseen training and sharing of guidelines and best practices as well as the creation of SPOCs should improve the quality and the treatment of requests. The streamlining of procedures and standards could increase effectiveness of voluntary cooperation channels.

These practical measures, which were widely welcomed by stakeholders, would to some extent improve the efficiency of the process: less resources would be spent on the process, and there would be an increase of the total number of requests made because requests that were not done previously because of the complexity of the process or a lack of knowledge about the procedure would now be done, thereby improving access to electronic evidence. This could in turn result in more effective investigations and prosecutions and contribute to improved deterrence for criminals, better protection of victims and improved security for EU citizens.

On the other hand, the room for improvement is limited by the shortcomings of the existing framework, or the absence of a framework. The measures in option A can only partly address the identified problems, as they cannot provide solutions to fragmented legal frameworks among Member States. The improvements to judicial cooperation channels would not fundamentally change the process, meaning that they will remain longer and more resource-intensive when compared to direct cooperation channels. Training and exchange of best practice could significantly improve the use of existing channels. For example, as reported in the EU-US MLA Agreement Review Report, direct cooperation has improved as regards providing content data in **emergency cases** such as those involving imminent risk of serious injury or death, including in terrorism cases. The usual process is that EU Member States' law enforcement authorities liaise with the U.S. authorities who, in turn, facilitate the voluntary provision by service providers of the required material pursuant to U.S. law. This arrangement has worked very well and, in the most exceptionally serious and urgent cases, the U.S. has assisted in the obtaining of evidence in under 24 hours. Under U.S. law, such voluntary

disclosure in emergency situations is accomplished without the need to meet the probable cause test. This improved cooperation is due at least in part to training, administrative cooperation and exchange of best practice. However, as can be deducted from the above description, these emergency procedures have strict conditions and are **highly exceptional**. They cannot be used for the large majority of number of cases where electronic evidence is needed in the framework of normal criminal investigations. While training and information to judicial authorities may lead to improvements in the use of MLAT channels, they cannot address the problems of bottlenecks on the US end, where authorities are overloaded by requests from all over the world. It is most unlikely that a situation where the number of direct requests outnumbers the number of MLATs by a factor of 10 would be dramatically overturned by such measures.

In addition, the US have little incentive in further investing in procedures which are not required under their laws and not necessary to protect sovereign interests. Under these circumstances, the practical improvements to the current system are naturally limited.

The practical solutions for direct cooperation would also not address the need for increased legal certainty, transparency and accountability in direct cross-border cooperation between authorities and service providers, which was highlighted as a key issue by all stakeholders in the expert process. Finally, the proposed measures on cooperation with service providers would only cover providers under US jurisdiction and be limited to non-content data. Therefore, while the overall impact on the effectiveness of criminal investigations should be positive, this measure by itself would not fully address the problem, as also highlighted by experts during the consultation.

**Option B: option A + international agreements**

The impacts of this option are the same as in option A, plus those of international agreements, described below.

A broadly applicable international regime, which could possibly also include the US, would be easier to implement for national authorities and service providers than many divergent regimes. The impact on the ability of public authorities to investigate and prosecute crime would depend on the concrete provisions negotiated and on the participating countries. Both judicial cooperation and direct cooperation could be improved. However, with an increasing number of countries involved, the likelihood of a shared understanding of the necessary conditions and safeguards decreases, and solutions are likely to be limited in scope.

Bilateral agreements could create more legal certainty on the basis and process for direct cooperation with private parties in non-EU countries, and allow for a tailor-made solution befitting both partners. An EU-US Agreement could allow service providers under US jurisdiction to provide content data to EU public authorities, which is currently not possible. This in particular could not be achieved by EU legislation alone, as – depending on the circumstances of the case – it could create a conflict of law with US law. Both bilateral and international agreements were therefore widely cited as good options by a range of stakeholders.

However, both bilateral and multilateral agreements are uncertain; it could take years, if at all, to reach an agreement, and the precise outcome is beyond the EU's control as it would also depend on the non-EU countries involved.

In conclusion, option B would possibly lead to improvements, but these improvements are highly uncertain and depend on a number of actors. Moreover, it is unlikely that the issues affecting the current legal framework would be adequately addressed by this option.

**Option C: option B + direct cooperation legislation**

The impacts of this option are the same as in option B, plus those of direct cooperation legislation described below.

European Production Order (EPO)

A measure allowing judicial authorities to compel certain foreign service providers to provide information, in a similar way to that of domestic providers, would bring significant benefits in terms of efficiencies both compared to judicial cooperation channels and to voluntary cooperation that exists with US providers on non-content data.

The major benefits of such a mechanism would be to provide a direct channel for the large majority of cases where the interest of the "receiving" country (from the judicial cooperation perspective) in the investigation is small to non-existent. It would accelerate the process compared to judicial cooperation tools, and create a mandatory framework compared to the current cooperation with US providers, which is voluntary from the perspective of US law. The European Production Order would be enforceable vis-à-vis service providers, meaning that the success rate would be significantly higher than under the current voluntary framework (where it is currently estimated to be below 50%). Because of possible cases of conflict with US law, it would not always allow EU judicial authorities to obtain content data. However, it is evident from the annual number of requests for non-content data to the US (around 120,000) as compared to the number of MLA requests, which must contain all requests for content data outside emergency situations (around 1,300), that the volume of non-content requests far exceeds those for content. Therefore, even if challenges persist when it comes to content data, the initiative would add significant value for a large proportion of requests.

With regard to EU providers, it would introduce a new mechanism, leading to a significant shift from judicial cooperation channels to more efficient direct cooperation channels.

Given that the proposed approach would represent a new step in judicial cooperation, amending existing instruments would not have the same effect. The closest instrument would be the European Investigation Order which has a different scope and cannot properly address the challenges on cross-border access to e-evidence in particular when it comes to deadlines and administrative burden. Overall, it would provide greater legal certainty and reduce the level of complexity and fragmentation for all stakeholders concerned. Authorities in particular welcomed this option in the consultation, but also service providers and civil society highlighted the need for a clear and certain framework with a robust set of guarantees.

The fact that the European Production Order would cover all forms of crime and not be limited to serious forms of crime would significantly improve the efficiency of the instrument.

It could be argued that such an option may create an incentive not to store data. However, this incentive is limited in impact as the current and future EU data protection and e-privacy frameworks already contain a data minimisation obligation: service providers are not to store data unless it is justified for certain specified purposes. In other words, data storage is determined by the purpose of the data processing and less by the possibility that a part of that data will be requested by police or judges in the framework of a specific crime investigation. Furthermore, the creation of a more effective channel to obtain electronic evidence from service providers is not expected to increase significantly the total number of requests.

The framework could also reduce issues experienced by authorities in some Member States with the admissibility in court proceedings of electronic evidence obtained through direct cooperation with service providers.

Overall, option C may result in evidence being obtained faster and evidence being obtained which public authorities would not even have tried to obtain currently because of the long delays or lack of legal basis. It would allow for a combination of the benefits for all types of measures covered by this option, as the measures are complementary, serve alternative purposes and address different problem drivers.

Improvements of judicial cooperation channels would still be useful and was highlighted as a key priority during the expert process: where the European Production Order would not help, e.g. in conflicts of law situations (content data with the US), judicial cooperation would prevail. For judicial cooperation among Member States, EIOs may still be issued to obtain e-evidence, e.g. when an investigating State needs different types of evidence form another Member State and requests it all in one go rather than choosing the European Production Order which would only work for part of the evidence. Any new instrument therefore should ensure coherence with the EIO and other procedures for judicial cooperation; this has been taken into account in the considerations. Often, however, the request for electronic evidence is an isolated one.

Some of the practical measures to improve cooperation between public authorities and service providers would to some extent become superfluous if the EPO came into force, as the legislation would establish a procedure, standard forms and an obligation to designate a legal representative. As this may take years, there would still be a benefit in the short term to introducing these practical measures on a voluntary basis. Furthermore, given that the scope of the measure is still not finalised, there may well be situations where such procedures would be necessary to obtain evidence. In addition, the training would be helpful in case of a change in legal framework because there would be a need to acquaint practitioners with the changes.

The international solutions complement legislative measures. In particular, once an agreement with the US was in place, removing conflicting obligations, the measure on cooperation with service providers could also allow authorities to obtain access to content data.

Access to WHOIS databases

Legislation providing for a legal basis to perform searches in the WHOIS database would enable authorities to continue to access the system in much the same manner as they currently do, even if some of its data elements should become password-protected and no longer

publicly available. Authorities specialised in cybercrime make look-ups to the WHOIS many times a day. Providing a new legal basis for the changed circumstances would preserve an essential tool in online investigations and would prevent a significant decrease in effectiveness of investigations, as highlighted by stakeholders in various forums (see Annex 12).

**Option D: option C + direct access legislation**

The impacts of this option are the same as in option C, plus those of direct access legislation described below.

The option to provide a legal basis for Member States to adopt legislation on direct access, subject to stringent conditions and safeguards, could improve the capacity of public authorities to investigate and prosecute crimes, both with regard to the time to obtain data and to the number of cases where e-evidence is successfully obtained. As highlighted by authorities, alternative judicial cooperation channels are not possible in all cases. Moreover, they would at times not be successful because of longer procedures. Putting in place a harmonised system of conditions and safeguards would provide a basis for enabling direct access in a manner that is mutually acceptable among Member States. By leaving the scope of measures in those Member States that already have efficient solutions in place largely untouched, the measure would not lead to any significant decrease in efficiency in those Member States.

Taken together, option C and direct access proposed would bring the most significant gain in terms of improving the capacity of public authorities to investigate and prosecute crimes. It would allow combining the benefits for all types of measures, as the measures are complementary, serve alternative purposes and address different problem drivers. This also applies for the two legislative measures, which address different situations and would, if combined, provide for a set of efficient tools to obtain cross-border access to e-evidence. A shift from judicial cooperation channels to these two tools can be expected for cases which do not necessitate involvement of another country, which would make access to e-evidence faster and more efficient. It would also respond to the calls from the Council and other stakeholders.

#### 6.1.2. Economic impact

The assessment of the economic impact of the different options focuses on the impact on service providers and public authorities impacted by the measures.

**Option O: baseline**

In the baseline scenario, the number of direct cooperation requests for non-content data is bound to increase. EU and US service providers will continue to receive requests for content data via judicial cooperation channels via their own judicial authorities, with numbers bound to increase here too in a similar order of magnitude as for direct cooperation. In both cases, service providers will either allocate additional resources to manage the increasing number of requests, or not, leading to an increase in the time to respond to such requests.

Public authorities are faced with a growing need for access to electronic evidence, which will further increase the number of requests, both using formal judicial cooperation channels and direct cooperation channels, and increase their costs. This was highlighted by authorities in particular throughout the consultation process.

Given the likely move of the WHOIS to credentialed systems, service providers could face an important rise in requests for access to subscriber information for domain names. This would create a significant additional burden both on courts and authorities in EU Member States and on the service providers, most of which do not yet have any procedures in place to deal with the expected increase in individually reviewable requests. Therefore, an important rise in costs both for internet infrastructure service providers and for national authorities is to be expected in the absence of action.

Legal fragmentation and legal uncertainty would remain and could act as a barrier to growth and innovation.

**Option A: non-legislative action**

Compared to the baseline scenario, the practical measures to enhance cooperation between public authorities in the EU and in the US would to some extent improve the quality of MLA requests submitted by EU authorities and would therefore generate efficiency savings for EU and US authorities. In particular the training of EU practitioners and the sharing of guidelines and best practices should have a positive impact, according to the experts consulted. The number of MLA requests from Member States to the US would likely increase slightly.

The development of the secure online platform would generate low costs for Member States who would connect to it, given that it is mostly financed from the EU budget. The platform itself would reduce costs for authorities requesting electronic evidence from another judicial authority in the EU using the EIO, by facilitating the creation and exchange of such requests.

The practical measures addressed to authorities to improve cooperation with service providers (SPOC, training, standardised forms, online portal) would generate some moderate costs for them[110], but also improve the quality of requests and would therefore lead to a net reduction of resources and costs for both service providers and public authorities. Those practical measures addressed to service providers (SPOC, streamlining of policies) would similarly generate moderate costs for service providers, in particular if changes to procedures have to be implemented, but public authorities would have a clear point of entry, reducing transaction costs, and would be faced with more consistent policies, meaning that they would not have to adapt to a variety of individual service providers' policies, leading to cost reductions for them. In addition, these practical measures may also lead to a slight shift from judicial cooperation channels to direct cooperation channels based on a better understanding by practitioners of this later channel, generating further savings, and to an increase of the total number of requests made via direct cooperation because requests that were not done previously because of the complexity of the process or a lack of knowledge about the procedure of a particular service provider would now be done. The overall benefit from the practical measures implemented by authorities should outweigh the costs, including those incurred by service providers that choose to implement practical measures on their side.

There would be a limited impact on non-EU countries, in particular as more requests use a more effective direct cooperation channel.

[110] The costs would vary depending on how Member States would implement this measure.

As the practical measures work within the present-day legislative framework, SMEs would be free to choose whether to participate or not in direct cooperation, given that there is no legal obligation to do so under US law. Within the EU, direct cooperation is not possible besides exceptional cases so there is no impact on SMEs. In the context of judicial cooperation, SMEs in the EU and beyond would likely stand to benefit from an increased quality of requests in the same manner as the larger providers.

**Option B: option A + international agreements**

The impacts of this option are the same as in option A, plus those of international agreements.

International solutions that would allow direct cooperation with service providers, be it in the framework of a multilateral or a bilateral agreement, could lead to a shift from judicial cooperation procedures to direct cooperation with service providers. Similar considerations regarding the economic impact on businesses and on public authorities would apply as for a measure on direct cooperation with service providers. Legal certainty could be improved and conflicts of law avoided in relation to the states that are party to the agreement, which could result in a reduction of burden and associated costs for service providers, as stakeholders highlighted during the consultation. A shift from judicial cooperation channels to a new form of direct cooperation and direct access instituted under any such agreement would likely apply to a greater extent in the framework of a bilateral agreement, given that the scope of a bilateral agreement is likely to be wider than in a multilateral context. This could be largely cost-neutral for service providers: the initial costs associated with the adaptation to any new legal framework could be offset by efficiency gains thanks to the reduction in complexity and number of laws applying to the same types of situations.

Any option including international agreements could have a similar favourable impact on non-EU countries as in Member States, as the agreement would define common approaches.

**Option C: option B + direct cooperation legislation (EPO + access to databases)**

The impacts of this option are the same as option B, plus those of the EPO and access to WHOIS databases.

<u>European Production Order (EPO)</u>

If an efficient procedure is implemented to obtain cross-border access to electronic evidence, a significant proportion of judicial cooperation requests would shift to direct cooperation as the more efficient instrument. This concerns predominantly intra-EU requests, as direct cooperation was previously not possible here, whereas a change in numbers regarding direct cooperation with US providers is not expected. Some shifts are to be expected from direct access as well, according to expert feedback. In addition, public authorities will attempt to obtain such data also in cases where today they may have been discouraged even to try due to the cumbersome procedure required, as practitioners explained. As a result, an increase in the total number of direct cooperation requests is expected.

The European Production Order would introduce additional burdens for service providers, but also benefits for them. European service providers would receive such requests directly from public authorities from other Member States, instead of from their own public authorities.

They would be subject to two sets of requests, domestic ones and European ones. This could possibly lead to uncertainty as to the applicable legal framework. To mitigate such risks, the proposal would introduce a unique form used by all public authorities throughout the Union for cross-border cases, to be translated into the language of the service provider. US service providers would benefit from a more harmonised legal framework for cross-border requests, instead of 28 different ones, and of increased legal certainty.

If the European Production Order would cover all forms of crime and not be limited to serious forms of crime, there might be an additional shift of requests to direct cooperation from judicial cooperation. The total number of requests they have to reply to would likely not change significantly, or only for those cases where public authorities decide not to pursue a case further because it would be too cumbersome to obtain the data via judicial cooperation.

The obligation to designate a legal representative in the Union would generate costs, in particular for service providers not established in the Union, who would have to mandate somebody in the Union to carry out this task. In particular for SMEs not established in the Union, there is a fear that this could represent an important burden[111]. On the other hand, this legal representative could be shared between service providers, and it could cover several functions (e.g. GDPR, ePrivacy and EPO), reducing the costs.

For public authorities, a legal framework for direct cooperation with service providers would improve efficiency, leading to a shift from judicial cooperation channels. When acting as issuing authority, public authorities would apply the same procedure, whether the service provider is established inside or outside of the Union, if they have jurisdiction under the proposal. Moreover, there would only be one authority involved, instead of two, as for judicial cooperation channels. This would reduce the costs for those authorities that otherwise would have had to recognise and execute judicial cooperation requests.

A combination of measures would result in cumulated cost reductions for both service providers and public authorities compared to the baseline scenario. The expected shift from judicial cooperation channels to cooperation with service providers could lead to important cost savings for judicial authorities both in the issuing and in the receiving State. Improvements in judicial cooperation channels, which, as explained above, would remain relevant in certain cases, could also result in some cost savings. Implementation of both practical and legislative measures would generate some costs for Member States, but these should be offset by the cost savings described above.

The biggest change for service providers offering services within the EU is that they would receive requests directly from public authorities in another Member State, rather than from their own public authorities via MLA or EIO channels. For those that participate in direct cooperation already, the main benefit would be the legal certainty and the harmonisation of procedures and forms of requests. For all service providers but particularly for SMEs, the

[111] For European SMEs, having to designate a legal representative as addressee of production orders may even bring benefits, as it would centralise expertise to deal with such orders.

nomination of SPOCs on the law enforcement side would make it easier (and cheaper) to authenticate EPOs.

Access to databases

If a solution is provided for access to WHOIS, authorities might be able to maintain the level of access they benefit from today, as the databases concerned are already in place. Therefore, costs would remain the same; there would be no additional costs generated by this proposal on the providers' side, and the same would be true for authorities. Costs generated by the planned changes to the WHOIS database system are independent of this proposal. The proposal would also prevent an avalanche of individual orders to service providers to produce the data, which might otherwise generate significant costs for both sides.

**Option D: option C + direct access legislation**

The impacts of this option are the same as in option C, plus those of the measure on direct access, which would not impose any new obligations or administrative burdens on service providers. For public authorities, there would be one-off costs for implementation of legislation. Over time, efficiency gains are to be expected because direct access involves fewer actors and is generally swifter, requiring fewer resources than judicial cooperation procedures in those situations where Member States would have chosen such alternative channels. However, because of the specific conditions for these kinds of measures, it is not expected that the cases will be numerous. Therefore the impact should be moderate.

This option should not have any effect on non-EU countries. Some non-EU countries may however object to foreign law enforcement accessing data stored in their territory.

6.1.3. Fundamental rights impact

The assessment of the fundamental rights impact of the different measures and options was carried out with particular attention, involving experts in fundamental rights and data protection, both inside the Commission and external stakeholders. The assessment included a dedicated meeting with data protection experts from the Member States and with the EDPS on 2 October (cf. Annex 2.2). The safeguards that are part of the legislative measures are the result of this assessment.

This initiative could affect the following fundamental rights:

- rights of the **data subject** whose data is accessed: right to protection of personal data; right to respect for private and family life; right to freedom of expression; right of defence; right to an effective remedy and to a fair trial;
- rights of the **service provider**: right to freedom to conduct a business; right to an effective remedy;
- rights of **EU citizens**: right to security.

**Option O: baseline**

In the baseline scenario, within the framework of public authorities' cooperation through EIO/MLA, the concrete protection of fundamental rights of persons whose data is sought will

continue to be ensured through national authorities acting under national and EU law, including the Police Directive and EU directives on procedural rights, such as the Directive on the right to information in criminal proceedings[112]. When applying the EIO Directive, the Charter of Fundamental Rights applies. For judicial cooperation channels, a double check takes place: at the level of the issuing authority, under the national law of the issuing State, and at the level of the executing authority, under the national law of the executing State[113].

Regarding the voluntary cooperation regime, the investigations and prosecutions are exclusively conducted in accordance with the national law of the investigating State, but the service provider may refuse based on the law applicable to it if that prohibits disclosing the data to foreign authorities (e.g. US law preventing the disclosure of content data to foreign authorities). For many Member States, national law authorises data requests to domestic service providers, but does not explicitly provide for the possibility to request data from foreign ones, which means that public authorities request such data from US providers in an uncertain legal environment.

Obtaining data under the current voluntary cooperation regime in the absence of a precise legal framework may affect the fundamental rights of the persons affected by the measure, including the right to an effective remedy, the right to respect for private life, and the right to the protection of personal data, as stakeholders also mentioned in the consultation. The Charter does not apply. In the absence of a clear legal basis, public authorities may be unable to make requests for direct cooperation that are in compliance with the Police Directive for law enforcement and in particular with Article 39, which sets specific conditions for such requests. Some US service providers verify the legality of a request for data, mostly with regard to the law of the issuing State, but they are private parties, not judicial authorities (who are the ones responsible). In the absence of a mandatory regime, the rights of service providers are not affected.

Direct access takes place in accordance with the national law of the investigating State, which regulates the conditions and safeguards applicable to the investigative measure such as the search and seizure. These vary between Member States, but as these investigative measures are among the most intrusive, there is generally a high level of protection. The Charter does not apply.

The problems affecting cross-border access to electronic evidence negatively affect the fundamental rights of persons who are or may become victims of crime (e.g. the right to life and dignity, and the right to property). This negative impact stands to increase with the growing need for cross-border access, in particular if publicly available data becomes available upon individualised request only.

**Option A: non-legislative action**

[112] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (OJ L 142, 1.6.2012, p. 1).

[113] Under the EIO Directive, the executing State can only refuse recognition and execution in a limited number of cases, but include fundamental rights issues. The possibilities to refuse are much wider under MLAT.

Compared to the baseline scenario, a very limited impact on fundamental rights may be expected with respect to cooperation between public authorities, if at all: The establishment of a secure online platform for authorities to exchange EIO/ MLA requests which ensures confidentiality of all data sets may have a positive effect on the protection of personal data. It would furthermore increase transparency and accountability and contribute to ensuring sound administration. There would be no change with regard to legal certainty and individuals' rights in the framework of voluntary cooperation with service providers.

The problems affecting cross-border access to electronic evidence would only be partially addressed through these measures, so the situation would still negatively affect the fundamental rights of persons who are or may become victims of crime (right to security). The negative impact would conceivably be less strong compared to the baseline.

**Option B: option A + international agreements**

The impacts of this option are the same as in option A, plus those of international agreements, described below.

International agreements may be advantageous, as they might allow ensuring an adequate level of protection of fundamental rights, including data protection. They could allow for a joint definition of mutually acceptable conditions, thus reducing conflicts of law, and specific mechanisms to ensure fundamental rights protection, possibly elevating international standards to the EU level. They would also contribute to legal certainty, which could have a positive impact on the right to security and the freedom to conduct a business. Given their wider geographical coverage, they would therefore add value compared to the previous options.

**Option C: option B + direct cooperation legislation (EPO + access to databases)**

<u>European Production Order (EPO)</u>

An EPO could potentially affect a number of fundamental rights of the affected persons. To ensure the protection of the rights of these persons, the measure includes the safeguards outlined in section 5. The intervention of a judicial authority when the order is issued would ensure that the legality of the measure has been checked and that the order does not unduly infringe on fundamental rights, including the effects of important legal principles such as the lawyer client privilege or protection of journalistic freedoms. As the measure would not include a limitation to serious forms of crime, the issuing judicial authority should be required to ensure in the individual case that the EPO is necessary and proportionate, including in view of the gravity of the offence under investigation. This would prevent that an EPO is issued in a situation where it would be disproportionate in view of the lack of seriousness of the offence, but avoiding at the same time that the instrument could not be used at all for certain types of crimes which may become important for other reasons in specific cases, e.g. because they affect a high number of victims. The judicial authority would also be required to check that the data category sought is necessary for and the request itself is limited to what is necessary for and proportionate to the purpose of the proceedings.

The possibilities of an effective remedy for persons whose data is being requested would also be addressed. Immunities and privileges of certain professions such as lawyers would also

have to be taken into account during trial in the issuing State, as highlighted by a number of stakeholders. The review by a judicial authority will serve as a further safeguard here.

Because the production order would be a mandatory measure, and it would also encompass the obligation to designate a legal representative, the measure could also affect the rights of service providers, in particular the freedom to conduct a business. Insofar that such measures could affect rights and freedoms of the service providers stemming from Union law, the proposal would include a right for the service provider to raise certain types of errors before a court or a tribunal in the issuing Member State, e.g. if the order has not been issued by a judicial authority.

One of the risks of a mandatory approach would be that it could inspire non-EU countries which do not have fundamental rights safeguards in place that can be considered comparable to those in the EU, including in the field of data protection, to introduce a reciprocal obligation for EU service providers active on their territory. This could undermine the high level of data protection ensured by the EU acquis, by making this data potentially available to such non-EU countries. This "model" role of EU law could be addressed in two ways: first, by providing a proposal that contains strong safeguards and explicitly references the conditions and safeguards already inherent in the EU acquis and can thus serve as a model for foreign legislation; and secondly, by including a specific conflicts of law clause that would allow service providers to identify and raise conflicting obligations they would be facing. This clause would give a role to the law of the non-EU country and include the possibility for consulting the authorities of that country on the existence of such conflicting obligations, and for taking their views into account in the decision on whether to uphold or annul the contested EPO. International agreements may further reduce conflicts of law situations. However, given that a number of non-EU countries have already implemented their own approaches to these matters, expectations as to the positive impact of any "model" role of EU law necessarily have to be limited. This is particularly true for the fundamental choice as to whether to address the challenges by imposing data localisation requirements, which this initiative seeks to avoid in view of the inherent negative side effects.

The above analysis suggests that, if applied with proportionality and complemented with the proposed safeguards, each measure in this policy option respects fundamental rights. On the other hand, by not including a measure on direct cooperation, or delaying its adoption, option C would leave direct cooperation to diverging national regimes, thereby not ensuring a similar high level of protection in the Union of direct access measures; safeguards would remain a national issue. Minimum safeguards could potentially stem from the additional protocol to the Budapest Convention, but it is too early to say. With a functioning mechanism to obtain data from service providers, it can be assumed that there would be fewer incentives for Member States to use direct access also in situations where they could instead go to a service provider.

Access to databases

The impact on fundamental rights of the legal base for access to dedicated database systems would be small as the data contained in this database is not particularly sensitive in nature and authorities' access would remain essentially unchanged. Creating such a legal base would also indirectly allow the system to move to a tiered-access model as it could still ensure the vital

public policy interests at stake. This in turn would have a positive effect on individuals' fundamental right to privacy, as their personal data would no longer be publicly available and access to it – especially for abusive purposes – would be limited in a more effective manner.

**Option D: option C + direct access**

The impacts of this option are the same as in option C, plus those of a measure on direct access, as described below.

This option would allow public authorities to access data that is not publicly available and that is, in most cases, personal data. However, the intrusiveness is already inherent in the national investigative measure, such as the search and seizure measure. Possible EU legislation instituting conditions and safeguards could inspire further EU Member States – beyond the 20 which already provide for direct access – to adopt legislation on these issues. A proposal would therefore indirectly have an impact on the rights of the target of the investigation. It would allow public authorities to also access data stored remotely if it is not clear whether it is stored on their territory, where this is not yet provided for in national law, i.e. it would widen the scope of the measure to data to which they may not necessarily have had access until now. But whether the data is stored on a device or remotely in the cloud, on the territory of the investigating Member State or in a non-EU country, should not be a relevant factor regarding the fundamental rights protection of the data subject (which should be ensured by the conditions and safeguards), nor regarding the sensitivity of access by public authorities.

As the measure would be anchored in national law, all safeguards and conditions set out by the respective national law would be preserved by this instrument (including thresholds and privileges). In addition, it would include additional conditions and safeguards to ensure that the use of this measure remains exceptional, such as the requirement that the data sought is necessary for the investigation and the measure is limited to what is necessary and proportionate to the purpose of the proceedings, also in view of the nature and gravity of the offence under investigation. It would therefore likely have a positive impact on the fundamental rights of the person affected as it could serve to limit overly broad national legal bases. It would also have a positive impact in creating legal certainty on the mutual acceptance among EU Member States of the respective national measures.

Again, there is a risk of reciprocal response by non-EU countries. At the same time, a number of non-EU countries would not need to rely on EU legislation, as they may have already put in place other approaches to ensure access to data, such as data localisation obligations or a more expansive set of investigative measures, including possibilities for investigators to directly access data, going further than what is proposed here. In that light, creating a framework for access to electronic evidence that builds on the robust protections already provided for under EU law and including specific safeguards could also set a positive example. Moreover, international agreements may reduce reciprocity issues, if they include agreements on direct access as is already the case – to a limited extent – under the Budapest Convention.

When assessing a combination of all measures, the main ones impacting fundamental rights are the legislative measures. As explained above, they would include sufficient safeguards to make them compatible with fundamental rights. A combination of all legislative measures,

including international solutions, would facilitate cross-border access to personal data to the biggest extent, and would also ensure that fundamental rights are most widely protected in all situations covered by these measures. If only some of these measures would be pursued by Union law, it would still leave room for either national unilateral solutions and/or voluntary cooperation outside of a clear legal framework. The legislative measures would also ensure that the practical measures can take place in a legal framework where fundamental rights are protected, thereby complementing the practical measures from a fundamental rights point of view.

In the Tele 2 judgement[114], the ECJ held that general and indiscriminate data retention legislation concerning metadata entailed a particularly serious interference with the rights to privacy and data protection and that the user concerned is, as a result, likely to feel that their private lives are the subject of constant surveillance. It could also, according to the Court, affect the use of means of electronic communication and thus the exercise by users of their freedom of expression. The scope of the two legislative measures is limited to a concrete investigation and not *in abstracto*, and therefore cannot be compared to a general data retention scheme. The interference with fundamental rights is justified by the aim of the measure, which is to ensure effective investigation and prosecution of crimes in the EU. This would be ensured in each individual case by the issuing judicial authority.

The above analysis suggests that, if applied with proportionality and complemented with minimum conditions and safeguards, the measures in this policy option respect fundamental rights.

### 6.2. **Quantitative assessment**

The quantification of the costs and benefits of the policy measures/policy options is limited by the **lack of data**, and requires the use of a number of **assumptions**, described in detail in Annex 4. Given these limitations, the estimates in this section provide an idea of the **order of magnitude** of costs and benefits and therefore should not be taken as exact forecasts.

This section summarises the quantitative assessment for each policy option by estimating:

- the main **administrative costs** for **Member States** (i.e. **transposition and enforcement** of the legislation) and **service providers** (i.e. **compliance** with the legislation), distinguishing between **one-off** and **continuous** (annual) costs.
- the main **benefits** (**savings**) due to:
    - a **reduction** of current **administrative costs**, for Member States and service providers; and
    - a possible **reduction of crime** caused by the stronger **deterrence** that a **more effective** investigation and prosecution of crimes could create, thanks to improvements in cross-border access to e-evidence.

[114] Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others (Joined Cases C-203/15 and C-698/15), paragraphs 101-102, 21 December 2016.

### 6.4.1 Costs

The costs of this initiative are purely **administrative**, i.e.:

| Costs = **cost/minute** of the person doing the tasks x **minutes** required to do the tasks |
|---|

- **Cost/minute**:
  - It includes:
    - the salary based on the median of the salaries in the EU of level 2 professionals in the International Standard Classification of Occupations (ISCO)[115];
    - non-wage labour costs such as employers' social contributions;
    - 25% overhead (i.e. expenses not related to direct labour, such as the cost of office equipment.)
  - The value is **30 EUR/hour = 50 cents/minute**.
  - It is assumed that this value remains **constant** for all options and over time.
- **Minutes** required to do a task:
  This value can change from option to option, in two ways:
  - the **time** required to do **one task** changes, or
  - the **total number of tasks** changes.

Considering the above, to calculate the costs of each option the following 5 questions where analysed for each of the measures:

1. Are there any **one-off costs**? (e.g. transposition of the legislation).
2. Does the measure **change** any of the **times** required to do **any task** required to attempt to access e-evidence across borders in each of the three channels (i.e. judicial cooperation, direct cooperation and direct access)?
3. Does the measure **change** the **total number** of **attempts** to access e-evidence across borders in each of the 3 channels?
4. Combining the above, does the measure **change** the **total time** to attempt to access e-evidence across borders?
5. Combining the above, does the measure **change** the **total continuous costs** to attempt to access e-evidence across borders?

Limitations

- The implementation of practical measures would be **voluntary** for both Member States and service providers, so it is not possible to provide accurate estimates of actual costs.
- The assumptions have a certain degree of approximation and subjectivity. To mitigate this, the **methodology, the model and the input data** were **discussed and validated with external experts and reviewers** in several dedicated meetings (focus groups). The experts included practitioners from both the private sector (service providers) and from public authorities in Member States.

[115] Based on 2014 Mean Hourly Earnings By Main Economic Activity And Occupation* + adjustment to 2014 Prices No data for Croatia was available. Source: Eurostat, Structure of Earnings Survey - NACE Revision 2.

- For international measures 3 and 4, because of the high degree of uncertainty regarding what would be agreed and when, it is not possible to quantify the impacts at all.

The tables below summarise the one-off and continuous costs estimates for the retained policy measures and the policy options they combine into (savings are indicated in red and with a minus sign):

*Table 7: one-off and continuous costs estimates for the retained policy measures (EUR)*

| POLICY MEASURES | ONE-OFF COSTS | | CONTINUOUS (ANNUAL) COSTS - BASELINE | |
|---|---|---|---|---|
| | Service providers | Public authorities | Service providers | Public authorities |
| 0 | € 0 | € 0 | € 0 | € 0 |
| 1 | € 0 | € 400,000 | € 448,345 | -€ 98,574 |
| 2 | € 120,000 | € 292,800 | -€ 1,479,387 | -€ 1,507,361 |
| 3 | NA | | | |
| 4 | NA | | | |
| 5 | € 1,560,000 | € 1,296,000 | -€ 924,385 | -€ 763,975 |
| 6 | € 0 | € 672,000 | -€ 2,241,725 | -€ 4,928,724 |
| 7 | € 0 | € 648,000 | -€ 134,503 | € 113,361 |
| **Total** | **€ 1,680,000** | **€ 3,308,800** | **-€ 4,331,656** | **-€ 7,185,273** |

*Table 8: one-off and continuous costs estimates for the policy options (EUR)*

| POLICY MEASURES | ONE-OFF COSTS | | CONTINUOUS (ANNUAL) COSTS - BASELINE | |
|---|---|---|---|---|
| | Service providers | Public authorities | Service providers | Public authorities |
| O | € 0 | € 0 | € 0 | € 0 |
| A (measure 1+2) | € 120,000 | € 692,800 | -€ 1,031,042 | -€ 1,605,935 |
| B (1 to 4) | € 120,000 | € 692,800 | -€ 1,031,042 | -€ 1,605,935 |
| C (1 to 6) | € 1,680,000 | € 2,660,800 | -€ 4,197,152 | -€ 7,298,634 |
| D (1 to 7) | € 1,680,000 | € 3,308,800 | -€ 4,331,656 | -€ 7,185,273 |

The Member States that are likely to be most impacted are Germany, UK and France, as the major issuers of requests (see section 2.1.1.) and Ireland as a major addressee of requests where a number of important service providers are established.

See **Annex 4** for further details on the model, the assumptions and the calculations.

### 6.4.2 Benefits

There are two types of benefits

- Savings in administrative costs:
  - They derive directly from the calculation of costs in the previous section.

When these costs are lower than those that would be incurred in the baseline scenario, they are **benefits.**

- All the options except the baseline generate savings, as shown in table 8 above.

- Reduction of crime:
  - To estimate how each policy option could reduce crime, the **qualitative scores** on the social impact (enhanced security through more effective fight against crime) obtained in the assessment of each policy option were **translated into percentages of decrease of crime**.
  - The qualitative scores range from -3 (baseline) to +3 (option D) (see table 9 below).
  - In the baseline (policy measure 0), it was assumed that there will not be any decrease of criminal acts and organised crime gains (0%).
  - The qualitative scores range of -3 to +3 results in a respective range of 0% to -3% change (decrease) of criminal acts and organised crime gains. This assumes that the **range of decrease of crime** due to increased deterrence thanks to the implementation of a given option would be between **0% and 3%.**
  - The range of qualitative scores for the policy measures was converted into a range of percentages taking the above into account, resulting in the following table:

*Table 9: one-off and continuous costs estimates for the policy options (EUR)*

| Qualitative score for social impact | Estimated decrease of crime |
|---|---|
| -3 | 0% |
| -2 | -0.25% |
| -1 | -0.5% |
| 0 | -0.75% |
| 1 | -1% |
| 2 | -1.25% |
| 3 | -1.5% |

  - It assumes a current level of **crime** of **1.5% of EU GDP**[116], i.e. EUR 222 billion, based on estimates from the United Nations Office on Drugs and Crime[117].

Limitations:

- For the benefits derived from a reduction of crime, the assumption on the conversion of the qualitative range into percentages of decrease of crime was used for the sole purpose of **comparing the options**. Therefore, the total value of benefits derived from a reduction of crime for a given policy option must be interpreted in relation to the other options, rather than as an **accurate estimate** of the actual reduction of crime that a given policy option would cause.

[116] EU GDP in 2016 amounted to EUR 14 800 billion at current prices, according to Eurostat.

[117] Estimates of the United Nations for global costs of organised crime, United Nations Office on Drugs and Crime, Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes: Research Report, Vienna, October 2011. See also a related fact sheet from UNODC here, and a study from the European Parliament Research Service study on Organised Crime and Corruption, Cost of Non-Europe Report, March 2016.

- The percentage for each policy option was the sum of the percentages for its policy measures. This could lead to an **overestimation** of the benefits, since some overlaps on the benefits can occur when developing/transposing legislation combining two or more legislative and/or non-legislative measures.
- The assumptions have a certain degree of approximation and subjectivity. To mitigate this, the **methodology, the model and the input data** were **discussed and validated with external experts and reviewers** in several dedicated meetings.

The tables below summarise the benefits for the policy options:

*Table 10: estimated benefits for the policy options (EUR billion)*

| POLICY OPTIONS | Qualitative score for social impact | Estimated decrease of crime | Benefits from reduction of crime |
|---|---|---|---|
| O | -3 | 0.00% | 0 |
| A (measure 1 to 2) | -2 | -0.25% | -0.555 |
| B (1 to 4) | -1 | -0.50% | -1.11 |
| C (1 to 6) | 2.5 | -1.38% | -3.05 |
| D (1 to 7) | 3 | -1.50% | -3.33 |

See **Annex 4** for further details on the model, the assumptions and the calculations.

## 7. HOW DO THE OPTIONS COMPARE?

### 7.1. Qualitative comparison

The options were qualitatively compared in two ways: in relation to a set of assessment criteria and in relation to the extent that they achieve the specific objectives.

Comparison through assessment criteria

The following criteria were used to assess the impacts of each policy option:

| Criteria | Rationale for the assessment |
|---|---|
| **Effectiveness/ social impact** | • Enhance security through capacity to investigate, prosecute, sanction and prevent crime:<br>o Reduced delays in access to cross-border digital evidence<br>o Ensured cross-border access to digital evidence where it is currently missing<br>o Improved legal certainty, transparency and accountability<br>o Possible reduction of crime |
| **Efficiency** | • Administrative costs for Law Enforcement and Judiciary;<br>• Administrative and compliance costs for service providers, including SMEs<br>• Regulatory burdens on business<br>• Cooperation between public institutions and private sector |

| | |
|---|---|
| **Competitiveness** | • Effect on business models chosen by service providers, in particular where data location and access to this data is an important factor for customers |
| **Fundamental rights** | • Protection of personal data<br>• Respect for private and family life<br>• Right to liberty and security<br>• Right of defence<br>• Right to an effective remedy and to a fair trial<br>• Freedom of expression<br>• Freedom to conduct a business |
| **Impact on international relations** | • Sovereignty<br>• Conflicts of law<br>• Reciprocity |

| **Score** | **Impact level** |
|---|---|
| +2.5 to +3.0 | Highly positive (e.g. the option is likely to result in substantial improvements of the capacity of public authorities to investigate prosecute crime) |
| +1.5 to +2.0 | Moderate positive (e.g. high cost savings, better protection of victims, broader investigation and prosecution capacity, etc) |
| +1 | Small positive (e.g. uncertain or indirect impact) |
| -0.5 to +0.5 | Very uncertain or insignificant |
| -1 | Small negative |
| -2 to -1.5 | Moderate negative |
| -3 to -2.5 | Highly negative |

The table below summarises the qualitative scores for each main assessment criteria and each option. All criteria were given the same weight. The detailed comparative assessment of all options can be found in Annex 4.

| **Criteria** | **O** | **A** | **B** | **C** | **D** |
|---|---|---|---|---|---|
| **Effectiveness/social impact** | -3 | -2 | -1 | +2,5 | +3 |
| **Efficiency** | -1 | -0,5 | +0,5 | +1,5 | +2 |
| **Competitiveness** | -1 | -1 | 0 | -1,5 | -1,5 |
| **Fundamental rights** | 0 | 0 | +2 | +1 | +1 |
| **Impact on international relations** | -1 | -0,5 | +2 | +1 | +0,5 |
| **Total** | **-6** | **-4** | **+3,5** | **+4,5** | **+5** |

Effectiveness/social impact

The least effective is the baseline scenario, which even leads to a worsening of the situation due to the growing relevance of electronic data, while the most effective is option D combining all the seven retained measures. There is an important difference in terms of

effectiveness between options including legislative measures and options not containing them, as the main problem to be solved is a regulatory failure. Non-legislative measures can therefore only lead to limited improvements within the existing legal framework.

Option B can improve the effectiveness in relation to option A depending on the international agreement reached, but it remains highly uncertain what the results would be and when they would become effective. The biggest added value could be achieved if international agreements complemented EU legislation, while adopting legislation would also help to define a common EU position on some of the key issues.

Option C would significantly increase the effectiveness of access to electronic evidence in different ways, as it would:

- ensure faster access compared to current judicial cooperation channels,
- bring increased legal certainty compared to current voluntary cooperation channels, and
- ensure access to content where there is no conflict of law.

Improving access for non-content data is a significant step forward, as this type of evidence is more frequently requested than content data (cf. the transparency reports by US-based service providers that mostly concern non-content data, as content data can only be provided in emergency situations). For content data held by US providers, the preservation of data by service providers under the new instrument would ensure that at least the content data is not lost while judicial cooperation channels are pursued. Moreover, by also covering content data and combining it with a conflicts of obligations clause, the instrument would be future-proof and might not need to be amended if an agreement with the US was reached on access to content data in the framework of a bilateral agreement.

Option D would be slightly more effective than option C, as it would add another tool that would be useful for practitioners in certain situations. This would in particular benefit those Member States that do not access data possibly stored outside of their territory.

Efficiency

Except for the baseline, all options would generate some administrative costs for public authorities but are expected to lead to even greater benefits in terms of savings, as the processes become more efficient through the different sets of measures and public authorities would be able to use the most efficient and appropriate channel available.

Options C and D would both lead to a significant shift from judicial cooperation channels to more efficient direct cooperation channels and, to a more limited extent, to direct access channels, leading to important cost savings for Member States. If an international solution includes provisions on direct cooperation, this would also apply.

For service providers, all options will similarly generate administrative costs, and also some savings when processes become more efficient, but less than for public authorities as they remain involved to the same extent for both judicial cooperation channels and for direct cooperation channels. The main burden for them would result from options C and D including a European Production Order, as they would be faced with orders from other Member States

authorities, and would have to establish a legal representative. The biggest gain for them would be an increase of legal certainty and less conflicts of law.

Competitiveness

Under the baseline and option A, companies would continue to suffer from the lack of legal certainty currently surrounding cross-border requests for electronic evidence, and from a risk of conflicts of law if Member States adopt diverging national solutions. The options including legislative measures would improve legal certainty for companies and reduce the risk of conflicts of law. Options C and D with provisions on a European Production Order score best in this regard, as companies would have a clear legal framework and as a result a better understanding of their obligations under that framework.

Options C and D with provisions on a European Production Order could however also impact the business models chosen by companies with regard to corporate customers. It would therefore be important to include a "controller first" clause in the proposal to mitigate this risk.

Fundamental rights

Non-legislative options would have a smaller impact on fundamental rights of data subjects since they don't change the way the existing cooperation channels function, but make them more effective, either by reducing the time it takes to obtain the data (without fundamental right impact) or by increasing the number of requests. However, compared to legislative options, non-legislative options can't achieve a similar level of protection when compared to the baseline scenario. The lack of a clear legal framework for direct cooperation creates a risk for fundamental rights of the persons whose data is sought, as they can't refer to clear protecting provisions. This can only be overcome by a legal framework with clear rules protecting fundamental rights. The need for an appropriate legal basis in the area of criminal law (*nulla poena sine lege*) and criminal procedural law is furthermore anchored in national constitutions.

Option B, with the inclusion of international agreements may have a positive impact on fundamental rights, by including provisions protecting fundamental rights and by improving legal certainty in a larger number of countries, compared to the Union, but the level of protection may be lower for multilateral solutions than for bilateral agreements.

Options C and D with provisions on a European Production Order and on direct access would have the biggest potential impact on fundamental rights by facilitating access by public authorities to personal data, but these impacts would be mitigated by including sufficient safeguards and conditions, as explained above in the description of measures. E.g., the involvement of a judicial authority that assesses the proportionality and the conformity with fundamental rights of the measure, and with legal remedies clearly spelled out, protects the fundamental rights of the persons affected better than the voluntary cooperation where law enforcement issues requests in an unclear legal framework with service providers assessing the legality of this measure. This means that these options score better, in terms of fundamental rights impacts, than the non-legislative options.

Impact on international relations

While non-legislative options would not have much impact on non-EU countries, Options B, C and D including international agreements would benefit international relations by providing a mutually acceptable framework for cross-border access to e-evidence. However, international agreements are uncertain and may take a long time to become effective.

Options C and D, with provisions on a European Production Order and on direct access that move away from data storage location, could trigger reciprocal responses by non-EU countries. For the EPO, this could be mitigated by a 'conflicts of law' clause.

### 7.1.2 Assessment with regard to meeting the specific objectives

Reduce delays in cross-border access to electronic evidence

All options address this specific objective, but to different degrees. While options A and B would lead to reasonable reductions in delays for both MLA/EIO and direct cooperation, legislative options C and D would lead to a shift from judicial cooperation to direct cooperation (or direct access), significantly reducing delays, as the latter channels are faster. By introducing deadlines for direct cooperation, options C and D could further reduce delays.

Ensure cross-border access to electronic evidence where it is currently missing

While it can be expected that non-legislative measures would lead to some improvements also in terms of ensuring access to electronic evidence where it is currently missing, options C and D could achieve this to a greater extent, as they introduce a more efficient procedure which includes obligations for service providers to give access to the data.

Improve legal certainty, protection of fundamental rights, transparency and accountability

Only options B, C and D with their legislative measures would be able to effectively achieve this specific objective, which is closely linked to the shortcomings of the current legal framework. Options C and D would achieve it to a better extent than option B, because the outcome of international agreements is uncertain. Option D would achieve this objective slightly better than option C, because it would also add legal certainty for the situations of cross-border access to e-evidence using direct access. The result of this assessment is consistent with the scores obtained by each of the options: options including legislative measures score far better than the non-legislative option A, and among the former, options C and D obtain the highest scores because of the uncertainty of international solutions.

## 7.2. **Quantitative comparison**

Overall costs

For the purpose of comparing the options and calculating overall costs, a period of 10 years (2017-2026) was considered. Over that period, the total of costs per option is the following:

*Table 11: comparative quantitative assessment of the policy options over 10 years (EUR)*

| POLICY OPTIONS | Total costs |
|---|---|
| O | € 0 |
| A (measure 1+2) | -€ 25,556,978 |
| B (measure 1 to 4) | -€ 25,556,978 |
| C (measure 1 to 6) | -€ 110,617,058 |
| D (measure 1 to 7) | -€ 110,180,487 |

The costs above are negative, which means that they are **savings** compared to the baseline.

Overall benefits

The overall benefits are those calculated in section 6.2. that derive from a reduction of crime (the benefits derived from administrative savings are already considered in Table 11 above). It is assumed that the overall benefits will be achieved over a 10 year period as well. The table below compares the estimated costs and benefits for the different options:

*Table 12: comparative quantitative assessment of the policy options (EUR million)*

| | O | A | B | C | D |
|---|---|---|---|---|---|
| Overall costs (savings) | 0 | -€ 26 | -€ 26 | -€ 111 | -€ 110 |
| Overall benefits | 0 | € 555 | € 1,110 | € 3,053 | € 3,330 |
| **Total (savings)** | **0** | € 581 | € 1,136 | € 3,163 | € 3,440 |

Given the limitations caused by the lack of data, the calculation of benefits as a reduction of crime was carried out for the main purpose of comparing the options. In consequence, the total value of benefits must be interpreted in relation to the other options, rather than as an accurate estimate of the actual reduction of crime that the preferred policy option would actually cause. In particular, the much higher potential benefits in relation to the costs of the options should not be taken at face value. That said, option D is the option that could offer comparatively more benefits in the form of reduction of crime, followed closely by option C.

## 8. PREFERRED OPTION

On the basis of the assessment, the preferred option identified is option D. Option D scores slightly better than option C, with a total score of +5.

Main advantages

Option D would effectively achieve the strategic objectives of the EU intervention since:

- A combination of all the measures in option D would bring the biggest improvements of the public authorities' capacity to investigate and prosecute crimes. It would allow combining the benefits of the various measures as these are complementary.
- A combination of all measures would contribute to legal certainty and transparency in direct cooperation with service providers. It could create robust measures to ensure accountability, including through judicial redress.

In particular, option D would provide a comprehensive framework for obtaining e-evidence in cross-border investigations as it would include a European Production Order which would

have a wide material and geographical scope, made more effective through the support of practical measures and international agreements, and a measure on direct access which would provide solutions for swift access to data in very specific circumstances.

A combination of the European Production Order including a conflicts of law clause that would give a role to the law of the non-EU country, and of international solutions would significantly reduce the risk of reciprocal responses from non-EU countries. The risk of conflicts of law for service providers which arise from diverging national solutions would decrease. There would also be cost savings and reduced burden for authorities, both in issuing and receiving States, including non-EU countries.

Main disadvantages

Improvements to judicial cooperation in the EU would not extend beyond what is feasible within the existing legal framework, meaning that the mutual recognition process would not be fundamentally changed, as the same 120-day deadline would still apply. Some of the practical measures to improve cooperation between public authorities and service providers would to some extent become superfluous once a legislative measure on EPO comes into force.

Because of conflicts with US law, the European Production Order would not allow EU authorities to obtain content data from US providers, and a bilateral agreement could take years. Thus for some time Member States' authorities would not witness significant changes as relates to content data and would still have to rely on the existing MLA channels, which can be improved only to some extent through practical measures.

Trade-offs

This option would enhance security but at a cost for service providers not established in the Union, particularly for SMEs, due to the introduction of the obligation to designate a legal representative. Also, the measures to facilitate direct cooperation may have a considerable impact on fundamental rights, as it would allow public authorities to access data that is not publicly available and that is, in most cases, personal data.

Fundamental rights

When assessing a combination of all measures, the main options impacting fundamental rights are the two legislative measures. The two measures would include sufficient safeguards to make the measures compatible with fundamental rights. In the Tele 2 judgement, the ECJ held that general and indiscriminate data retention legislation concerning metadata entailed a particularly serious interference with the rights to privacy and data protection and that the user concerned is, as a result, likely to feel that their private lives are the subject of constant surveillance. It could also, according to the Court, affect the use of means of electronic communication and thus the exercise by users of their freedom of expression. In the framework of the two legislative measures, it cannot be excluded that a similar effect could be claimed in individual cases, but because the measures always take place in the framework of a concrete investigation and not in abstracto, it cannot be compared to a data retention scheme. The interference with these fundamental rights is justified by the aim of the measure, which is to ensure effective investigation and prosecution of crimes in the EU. This would also have to be ensured in each individual case by the issuing judicial authority.

Subsidiarity

Given the international dimension of the problems to solve, the measures included in the preferred policy option need to be adopted at EU level in order to achieve the objectives. In particular, action by Member States would fall short in addressing, e.g. the following issues:

- Different practices and legislative instruments at national level on cross-border access to e-evidence in order to enhance cross-border cooperation and ensure coherence in law enforcement approach to access to e-evidence;
- Improving the expediency of judicial cooperation on the basis of existing EU legislation, notably via the EIO;
- Obstacles to cross-border cooperation in obtaining e-evidence with non-EU countries.

Given the diversity of legal approaches, the number of policy areas concerned by the matter (security, fundamental rights including data protection, economic issues) and the large range of stakeholders, the EU seems the most appropriate level to address the identified problems.

Proportionality

The legislative instrument would introduce conditions and safeguards for judicial authorities of Member States to request from a foreign service provider through a European Production Order the disclosure of information stored in a digital form that could be used as evidence, including on proportionality, and conditions and safeguards for direct access to e-evidence from an information system on the basis of national laws. On the whole, the option does not go beyond what is necessary to achieve the objective identified for the EU intervention.

## 9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

The proposal should contain a commitment for the Commission to submit a **report** to the **European Parliament and to the Council** assessing the situation **2 years** after the deadline for transposition, and to evaluate the effectiveness, efficiency, relevance, coherence and EU added value **5 years** after the deadline to ensure that there is a sufficiently long period to evaluate after full implementation in all Member States. It will include a public consultation and possibly a survey of stakeholders to review the effect of the potential legislative act on the different categories of stakeholders.

To limit the additional administrative burden on Member States or the private sector due to the collection of information used for monitoring, the proposed indicators on the table below rely on **existing data sources** (e.g. transparency reports) whenever possible. Where no data exists, the preferred option contains a requirement for Member States to **systematically** collect data on the time from demand to access, the percentage of requests fulfilled and other data related to the implementation of the European Production Order. The **costs** of this data collection were included in the analysis of the options.

The Commission will conduct **targeted surveys** as indicated in the table below, assisted by Europol and Eurojust as needed. The costs of these surveys should be borne by DGs HOME and JUST within their operational expenditure (e.g. as support expenditure for operations of the Cybercrime policy area). The surveys will be conducted at least twice, coinciding, if applicable, with the reporting requirements for the Commission on the transposition and implementation.

In addition, the Commission will remain in close contact with the Member States and with the relevant stakeholders (in particular service providers) to monitor the effects of the possible legislative act. The following **fora** will be particularly relevant to gather qualitative evidence on concrete cases:

- Eurojust, and in particular the **European Judicial Cybercrime Network**[118], to exchange information with **judicial authorities**;
- the European multidisciplinary platform against criminal threats (**EMPACT**), part of the EU Policy Cycle, to exchange information with **law enforcement**;
  the **EU Internet Forum**[119], to exchange information with **service providers and public authorities in Member States** (Home Affairs Ministries).

[118] See here for more information.
[119] See here for more information.

*Table 13: monitoring of general, specific and operational objectives*

| | Objectives | Monitoring indicators | Sources of data and/or collection methods | Data collected already? | Actors responsible for data collection | Target |
|---|---|---|---|---|---|---|
| General | Ensure effective investigation and prosecution of crimes in the EU by **improving cross-border access to e-evidence** through **enhanced judicial cooperation** in criminal matters and an **approximation** of rules and procedures | **Percentage** of crimes that **cannot** be effectively investigated and prosecuted in the EU due to challenges in accessing e-evidence across borders | **Biannual survey** of public authorities in Member States | Yes (see section 2).<br>To be collected systematically | European Commission, with the collaboration of Member States | **<10%** |
| Specific | **Reduce delays** in cross-border access to electronic evidence | **Time** from **demand to access** (i.e. time required to access e-evidence from the moment the request to access it is issued), by type of:<br>• channel (formal/direct cooperation),<br>• data (content/non-content)<br>• situation (emergency/non-emergency) | **Systematic references** in **investigative file** to the point in time when the request is issued and when the answer is received systematic | No | • Member States' judicial authorities, and law enforcement (collection);<br>• European Commission (consolidation) | • Emergency: **<24h**<br>• Non-emergency: **<1 week**,<br>for both judicial and direct cooperation, and any type of data |
| | **Ensure** cross-border **access** to electronic evidence where it is **currently missing** | **Percentage of requests** to cross-border access to e-evidence that are **not fulfilled** | • **Systematic references** in **investigative** file if the request to access was denied<br>• Transparency reports | Yes (see section 2).<br>To be collected systematically | | **<10%** |
| | Improve **legal certainty, transparency and accountability** | **Percentage of respondents** (public authorities and service providers) that consider **these issues** as **obstacles** for cross-border access to e-evidence | **Survey** of public authorities in Member States and service providers targeting EU | | European Commission, with the collaboration of Member States | **<10%** |
| Operational | Enhance **operational** aspects of cross-border access to criminal evidence in criminal matters | **Number** of Member States with **SPOC** on both the public authorities and (main) service providers side | **Survey** of public authorities in Member States | Yes (see section 5).<br>To be collected systematically | | **All** Member States |
| | | **Percentage** of providers targeting the EU with their services with a **legal representative** appointed | | No (EPO does not exist yet) | • Member States' judicial authorities, and law enforcement (collection);<br>• European Commission (consolidation) | **>80%** |
| | | **Number** of **EPOs issued** | | | | **Main tool** to access e-evidence across borders by **2020** |
| | | **Percentage** of **EPO compliance** | | | | **>80%** |
| | | **Percentage of EPOs leading to sanctions** | | | | **<10%** |
| | | **Percentage** of **EPOs challenged in court** | | | | **<10%** |

**ANNEX 1: PROCEDURAL INFORMATION**

## 1. Lead DG, D*E*cide Planning/CWP references

- Lead DG: the Directorates-General for Migration and Home Affairs (HOME) and for Justice and Consumers (JUST) are the joint DGs for the preparation of this initiative.
- Decide reference: PLAN/2017/1416.
- CWP reference: this initiative appears in CWP 2018 under action 16 'Completing the Security Union': a proposal to improve cross-border access of law enforcement authorities to electronic evidence (legislative, incl. impact assessment, Art. 82 TFEU, Q1 2018).

## 2. Organisation and timing

Chronology of the IA:

- The consultation activities that inform the impact assessment started with informal consultations in April 2016 and continued with formal consultations until November 2017.
- In its June 2016 Conclusions on improving criminal justice in cyberspace[120], the Council asked the Commission to explore possible solutions, including legislative options, to improving cross-border access to electronic evidence. Specifically, the Council called on the Commission to take concrete actions based on a common EU approach to make mutual legal assistance more efficient, to improve cooperation between Member States' authorities and service providers based in non-EU countries, and to propose solutions to the problems of determining and enforcing jurisdiction[121] in cyberspace. The Council requested the Commission to report on intermediate results by December 2016 and to present deliverables by June 2017.
- The Commission subsequently announced an initiative on access to electronic evidence in its 2017 Work Programme[122] and launched an **expert consultation process** in July 2016 to **define the problem, set objectives and explore possible solutions**. This process involved relevant stakeholders, including Member States' experts, representatives of non-EU countries, representatives of industry associations, service providers, civil society organisations, practitioners and academics. The process started with bilateral meetings and small groups and progressively expanded, as options were developed and tested.
- The Commission presented a first progress report on this process[123] at the 8 December 2016 Justice and Home Affairs (JHA) Council meeting, and a non-paper on the results of

[120] Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST9579/16.

[121] In this document, the term "enforcing jurisdiction" makes reference to the competence of the relevant authorities to undertake an investigative measure.

[122] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme 2017, Delivering a Europe that protects, empowers and defends, COM(2016)710 final.

[123] Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, ST15072.

the expert consultation process[124] was presented at the 8 June 2017 JHA Council meeting, together with a more detailed technical paper[125]. The papers presented the conclusions from the expert process, setting out a detailed problem definition and proposing a combination of practical and legislative measures to respond to the problems identified.

- At the 8 June 2017 JHA Council meeting, Ministers asked the Commission to proceed with the implementation of the complete set of practical measures presented and to come forward with concrete legislative proposals both on direct cooperation with service providers and on direct access, on the basis of the considerations set out in the papers. In response, Commissioner Jourová announced that the Commission would propose legislative measures in early 2018[126].
- The Commission published an Inception Impact Assessment[127] on 3 August 2017. A public consultation was launched at the same time and stakeholders and citizens had the opportunity to express their views in an open public consultation through an online questionnaire that was accessible for 12 weeks, until 27 October 2017.
- The feedback from the expert process and its output, summarised in the above documents, were used as the base to build the impact assessment. Therefore, the problem definition, the policy options and the impacts reflect the views of the relevant stakeholders that participated in the expert process as well as in the other consultation activities detailed in Annex 2.
- The drafting of the impact assessment started in September 2017 and continued until December 2017, after incorporating the feedback from the RSB.

Joint HOME/JUST task force on e-evidence

- A joint task force HOME/JUST was set up at the end of 2015 to work on this initiative.
- It included members from the HOME Cybercrime unit and DG JUST's units responsible for procedural criminal law, fundamental rights policy, data protection and international data flows and protection.

Inter-service group (ISG)

- An ISG chaired by HOME and JUST, was set up in June 2017.
- The following DGs participated in the ISG: the Secretariat-General (SG); DG Informatics (DIGIT); DG Communications Networks, Content and Technology (CNECT); Legal

[124] Non-paper from the Commission services: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward. This document was prepared by the Commission services and cannot be considered as stating an official position of the Commission.

[125] Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace. This document was not adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

[126] More information here.

[127] Inception impact assessment: Improving cross-border access to electronic evidence in criminal matters.

Service (SJ); and DG TRADE. DG GROW, DG COMP and EEAS were invited but did not attend.

- The ISG met five times between June and November 2017. Discussion included the inception impact assessment, the questionnaire for the public consultation and the various drafts of the impact assessment.

## 3. Consultation of the RSB

The Regulatory Scrutiny Board received the draft version of the present impact assessment report on 22 November 2017. It issued an impact assessment quality checklist on 8 December 2017 with a number of very helpful comments. A detailed response to the RSB quality checklist was sent in advance to the RSB meeting on 13 December 2017, which specified how each of the RSB comments would be incorporated to the final version of the impact assessment.

The RSB issued a positive opinion on 15 December 2017, with a number of recommendations that completed the previously issued quality checklist. All of the RSB comments were incorporated into the final version of this document. The recommendations described in the RSB opinion were incorporated as follows:

| RSB comment | How it was incorporated in the IA |
|---|---|
| **(1) Context and complementarity with other instruments** | |
| The policy context could include additional references to relevant elements that triggered and contributed to shaping this initiative. It could further describe how and to what extent discussions in different fora have helped to scope this initiative. In particular, it should refer upfront to the measures for improving cooperation among judicial authorities and with service providers, identified as a result of the Commission's expert process and supported by the JHA Council of 8-9 June 2017. | References to relevant elements were expanded in the introduction, in sections 3.2 and 3.3 (Why should the EU act?). |
| The report should further explain how and to what extent the proposed measures complement others, such as the EIO, the negotiations of an additional protocol to the Budapest Convention or the revised EU-US MLA Agreement. Such clarifications could address questions of timing, scope and depth of these different instruments. The baseline scenario should reflect relevant | The complementarity between different measures (in particular EIO Directive, negotiations of an additional protocol to the Budapest Convention) was clarified in sections 2.2.1 and 5.4.4, Annex 4 section 1 and Annex 5 section 1 (for the EIO), additional explanations on how the 2016 EU-US MLA Review relates to the current initiative were added in section 2.3 and the |

| | |
|---|---|
| developments that are likely to occur independently of the adoption of the proposed measures, including changes to the Budapest convention. | baseline scenario was revised to better reflect likely developments regarding the Budapest Convention in the absence of EU legislative action. |
| **(2) Fundamental rights**<br><br>The report should provide a more complete discussion of fundamental rights issues surrounding the proposed measures, and appropriate safeguards.<br><br>The report should clarify interlinkages between the 7 measures of the preferred option. The report should further clarify the impact of delaying new legislation on the safeguards on direct access related to serious crimes in comparison to the EPO that covers all types of crimes. It should also explain any risks of not including in the package the intended legislation with conditions and safeguards for direct access. The report should discuss how this would affect, for example, the effectiveness, proportionality and balance of the initiative. | The discussion of fundamental rights issues in the report was complemented in various places (sections 5.2.2, 6.1.3 and 7.1, Annex 4 sections 1 and 2); in particular, the interlinkage between the 7 measures of the preferred option was clarified, and in the discussion of option C, considerations were added concerning the consequences of not covering or delaying a measure on direct access for fundamental rights. Because the initiative on direct cooperation will also be limited to certain forms of crime, it was not discussed specifically the impact of delaying legislation on the safeguards on direct access related to serious crimes in comparison to a measure on direct cooperation that would cover all crimes. |
| **(3) Stakeholder views**<br><br>The report should more systematically attribute the evidence and views expressed to the stakeholders that provided them. Clearer links between the feedback from stakeholders and the analysis would inform the reader about the degree of consensus surrounding the options and their likely impacts. This is especially relevant for businesses for which the analysis projects major savings in spite of increased data requests that they are likely to have to process as a result of the expected shift from legal assistance to direct cooperation with service providers. | A more detailed attribution of the views to the different types of stakeholder was added to Annex 2, including the views of service providers concerning the potential benefits.<br><br>Additional references to how the views of the stakehodlers were taken into account were added to Annex 1. |
| **(4) Flowcharts**<br><br>The report could usefully provide additional non-technical information on the proposed workflows for data sharing, highlighting the key differences that the measures would introduce. Such visual representations could cover the main distinctions between different types of data sharing such as content vs non-content or intra vs extra EU | Flowcharts were added in section 5.2.2 and in Annex 4, Measure 5 to compare the current procedures and new measures and to illustrate how access to different data categories might function, as well as delivery of the order. All measures set out here grant access to evidence that could in theory also be obtained through other procedures which however are |

| | |
|---|---|
| exchanges. It should differentiate measures in the final package according to whether they grant access to new evidence or faster access to evidence that can already be accessed with existing procedures. | deemed to be not appropriate in view of requirements. The initiative proposes not to differentiate according to data storage location intra or extra-EU. |

The impact assessment for this initiative was discussed briefly in a bilateral meeting between Matthias Ruete (Director General at DG HOME) and the RSB on 29 September 2017. A draft intervention logic was shared in advance of the meeting. During the meeting, the RSB underlined the importance of:

- Providing an overview of what the costs might be that allows the College to understand the trade-offs and implications of choosing a particular option
- Subsidiarity: ensure that there is a real value added in EU intervention that does not duplicate existing efforts in the Member States (in particular with regard to practical measures).
- Proportionality: ensure that EU intervention is limited to the objectives set and that these are in coherence with the legal basis.

## 4. Evidence, sources and quality

As mentioned above, the expert consultation process that ran from July 2016 to October 2017 was one of the main **sources of evidence** used in the impact assessment.

Other sources of evidence included:

- the other consultation activities (surveys, other meetings and conferences) described in detail in Annex 2. Whereas the various surveys were an important source of data, given the limited number of responses in some of them and to ensure their validity and representativeness, the surveys were complemented with other sources of information, such as meetings (e.g. expert meetings, bilateral meetings) and conferences.
- the transparency reports of major service providers, used to complement the analysis of the size of the problem (see Annex 11);
- a large number of studies have been conducted on the problem of access to evidence across borders, including the recently concluded and EU-funded EVIDENCE project[128].
- a number of other actors have also made finding solutions to these and related problems a key priority and are actively working on them in parallel processes. This enabled the Commission services to build on input and previous reflections from a variety of sources, including the Council of Europe (Cloud Evidence Group), Interpol, bilateral and unilateral efforts at Member States' and non-EU countries' level, academic research and many conferences. The Commission services have sought to

[128] See here.

ensure close coordination of their work with efforts under way elsewhere and have also benefited from the expertise of Europol and Eurojust.

- the impact assessment also drew on results of previous work in the EU, notably on the March 2016 Amsterdam conference on Crossing Borders: Jurisdiction in Cyberspace organised by the Netherlands Presidency of the Council of the EU, and on the first results of the Council of the European Union Working Party on General Matters including Evaluation (GENVAL) 7th Round of Mutual Evaluations on Cybercrime.

The above evidence supports the quantitative and the qualitative assessment of impacts in the report. In particular, the stakeholder consultation focused on establishing the precise nature of the existing challenges before turning to possible ways to address these challenges. The possible options were checked and re-checked with stakeholders at each step of the process (for example, a first problem definition was published in December 2016 and refined based on input from all stakeholders). Throughout the consultation, close coordination was sought with other actors currently working on the same or similar issues from different perspectives, such as the Council of Europe Budapest Convention Secretariat, the U.S. Department of Justice, the Internet & Jurisdiction project and a number of academics, to ensure coherence and compatibility of solutions put forward.

The impact assessment made an effort to properly reference all the sources, review their **quality** and include hyperlinks whenever possible.

The calculations of costs and benefits were limited by the lack of data. The Commission made significant efforts to collect data, or at least estimates, from public authorities and service providers through targeted surveys. Where this information was not available, assumptions were made in the model to calculate costs, which were validated with external experts from Member States and service providers.

**External expertise** was gathered through the stakeholder consultation as explained in detail in Annex 2. Also, a contractor was engaged to help gather data on costs and benefits from public authorities in Member States and service providers, which was used in the model to estimate the costs of the various options (see annexes 3 and 4).

## ANNEX 2: STAKEHOLDER CONSULTATION

This annex is the synopsis report of all stakeholder consultation activities undertaken in the context of this impact assessment. It has 3 sections:

1) Consultation strategy.
2) Results of the consultation.
3) How the results have been taken into account.

### 1) Consultation strategy

The consultation had four main **objectives:**

- to identify current best practice, as well as challenges and gaps, and the relevant needs of all stakeholders;
- to identify ways forward with the help of stakeholders that would best address those needs;
- to ensure that stakeholders (including citizens and those who would be directly affected by this initiative), can provide their views and input on the possible options for the way forward; and
- to improve the overall evidence base underpinning the initiative.

The consultation was structured as follows:

1. **Who** – **stakeholders** consulted:
    - citizens;
    - service providers:
        - individual companies;
        - professional and business associations;
    - public authorities from Member States and relevant non-EU countries:
        - Ministry of Justice officials;
        - Ministry of Interior officials;
        - law enforcement representatives;
    - legal practitioners (lawyers, prosecutors, judges);
    - non-governmental organisations (NGOs);
    - inter-governmental organisations (IGOs);
    - EU institutions and agencies; and
    - academia.

2. **How** – **methods and tools** used:
    - **Surveys**:
        - **Open public consultation**:
            - Survey open to feedback from **any interested party**.
            - Open for **12 weeks**, from 4 August 2017 to 27 October 2017.
            - It included a link to the Commission website on cross border access to e-evidence[129], which provided further information.

[129] Accessible here.

        - The **consultation on the Inception Impact Assessment**[130] was launched at the same time as the open public consultation. Any interested party could provide feedback on the Inception Impact Assessment from 4 August 2017 to 31 August 2017.
    - **Targeted** surveys:
        - Survey of **public authorities** in Member States on **current practices** concerning the different channels to cross-border access to e-evidence, carried out between 26 July 2016 and 16 September 2016; the last responses from Member States were received on 28 February 2017.
        - Survey of **public authorities** in Member States on the **size of the problem**, carried out between 6 October 2017 and 23 October 2017.
        - Survey of **public authorities** in Member States on **costs and benefits** associated with the different options, carried out between 25 October 2017 and 8 November 2017.
        - Survey of **service providers** on **costs and benefits** associated with the different options, carried out between 25 October 2017 and 8 November 2017.
- **Meetings**:
    - **Group** expert meetings:
        - Expert meetings organised by the Commission in a process that gradually included a wider range of stakeholders (public authorities from member States, service providers, civil society, academia, etc.)..
        - Expert meetings organised by other entities, including the Council of Europe, the European Judicial Cybercrime Network and the European Union Chiefs of Cybercrime Units (EUCTF).
    - **Bilateral meetings:**
        - Meetings with a wide range of stakeholders organised at the initiative of the Commission or the stakeholders.
        - Meetings with non-EU countries potentially affected by EU legislation in this area, with a focus on the US as the key country in this context.

    These meetings are collectively referred to in the impact assessment as the "expert process".
- **Conferences**:
    - The Commission participated in a number of conferences that included discussions on cross-border access to electronic evidence. The Commission presented its work in this area, gathered feedback on the initiative from other conference participants and invited additional participation in the expert process and the public consultations.

| |
|---|
| In total, the **consultation activities** lasted more than **1.5 years**, from **April 2016 to November 2017**. |

[130] Accessible here.

The consultation was designed to follow the same logical sequence of the impact assessment, starting with the problem definition and allowing for a **gradual development** of the possible options and scenarios and their impacts, gradually increasing the number of stakeholders involved.

3. **What –** the consultation gathered feedback on the **problem definition, options and impacts** of these options, based on the three channels to access e-evidence across borders: **judicial cooperation, direct cooperation and direct access**.

The table below summarises the structure of the consultation:

*Table 1: consultation strategy for improving cross-border access to electronic evidence*

| | | **HOW** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Surveys | | | | | Meetings | | Conferences |
| | | Open public consultation | Targeted survey 1 | Targeted survey 2 | Targeted survey 3 | Targeted survey 4 | Group | Bilateral | |
| **WHO** | Citizens | ✓ | | | | | | | ✓ |
| | Service providers | ✓ | | | | ✓ | ✓ | ✓ | ✓ |
| | Public authorities | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| | Practitioners | ✓ | | | | | ✓ | ✓ | ✓ |
| | NGOs | ✓ | | | | | ✓ | ✓ | ✓ |
| | IGOs | ✓ | | | | | ✓ | ✓ | ✓ |
| | EU institutions and agencies | ✓ | | | | | ✓ | ✓ | ✓ |
| | Academia | ✓ | | | | | ✓ | ✓ | ✓ |
| | | Problem definition and options | Problem definition and options | Size of the problem | Costs and benefits | Costs and benefits | Problem definition, options and impacts | Problem definition, options and impacts | Problem definition, options and impacts |
| | | **WHAT** | | | | | | | |

## 2) Results of the consultation

The following sections present a summary of the main results of the consultation activities.

Open public consultation

The increasing use of information society services are perceived as a challenge to the work of law enforcement and judicial authorities by **nearly half** of the public survey respondents[131]. In their comments, respondents repeatedly identified following aspects relevant to criminal investigation:

- the borderless nature of the internet;
- the use of encryption;
- anonymity;
- ongoing technological development; and
- insufficient technological equipment of law enforcement authorities.

When accessing cross-border e-evidence, law enforcement and judicial authorities face various obstacles. The **lengthy process** to finally receive or access the evidence through judicial cooperation was marked as the most common complication[132] by practitioners from law enforcement and judicial authorities. The respondents have also identified difficulties to determine where data is stored[133], difficulties to obtain electronic evidence when the service provider in question has outsourced its computing resources[134], and unpredictability of responses by the service provider when the request in not mandatory[135] as "very relevant" or "relevant" issues complicating investigations where electronic evidence is concerned.

With regard to concerns about a possible negative **impact on rights**, which is a relevant issue for most of the public survey respondents[136], specific safeguards to guarantee fundamental rights are perceived as a necessary condition for any cross-border instrument to access electronic evidence. The respondents expect the initiative to provide for higher level of legal certainty[137] and these guarantees. Furthermore, a limited number of offences on which a direct access would apply, notification to the authorities of the other Member State or their approval, necessity and proportionality, prior judicial authorisation, effective oversight, and legal remedies for the person affected are amongst the necessary attributes of this instrument, according to the public survey respondents.

---

131 Open public consultation feedback: 46.3% yes, 37.8% no, 15.9% no opinion (n=82) of all respondents.

132 Open public consultation feedback: 96% (n=25) of the respondents from law enforcement, judicial or public authorities directly related to it (e.g. Ministry of Justice, Ministry of Interior) selected "very relevant" or "relevant".

133 Open public consultation feedback: 88% (n=25) of the respondents from law enforcement, judicial or public authorities directly related to it (e.g. Ministry of Justice, Ministry of Interior).

134 Open public consultation feedback: 96% (n=25) of the respondents from law enforcement, judicial or public authorities directly related to it (e.g. Ministry of Justice, Ministry of Interior).

135 Open public consultation feedback: 84% (n=25) of the respondents from law enforcement, judicial or public authorities directly related to it (e.g. Ministry of Justice, Ministry of Interior).

136 Open public consultation feedback: 82.05% (n=39) respondents answering in their personal capacity selected "very relevant" or "relevant".

137 Open public consultation feedback: 74.67% (n=75) of all respondents who answered this question.

Possible harmonisation of definitions related to cybercrime in the context of judicial cooperation was supported by the vast majority of public survey respondents[138] who are practitioners in law enforcement and judicial authorities or service providers. Nonetheless, the above mentioned legal definitions should be introduced in accordance with the dynamic and complex nature of internet, thus not to limit the law enforcement and judicial authorities and not to establish unnecessary obstacles to effective criminal investigations. Yet, there was no consensus on whether the EU initiative should only set up a legal framework for cases with cross-border dimension or whether it should also cover purely domestic cases.[139]

**Service providers** also experience difficulties when receiving and processing cross-border data access requests. The time-consuming assessment of legality and legitimacy of such requests, a need to contact the issuing authorities in order to obtain further information and lack of common definition of requested data leads to additional costs which are borne by the private entities. Furthermore, in certain cases the verifications necessary to ascertain the authenticity and legitimacy of the request might require contracting an external counsel or other third party vendor. An EU initiative on electronic evidence expected to achieve a higher degree of legal certainty would therefore allow **for more time and cost-efficient way** to provide the requested data. Requests differing in form and content between Member States are also considered a serious driver for costs[140], yet an EU-wide common request form is not expected from the initiative by service providers[141].

Practitioners from **law enforcement authorities** or public authorities directly related to it expressed their support to an EU initiative in the area of electronic evidence as they expect the initiative to achieve a higher standard of legal certainty[142] and easier cost-efficient access to the evidence by a streamlined EU-wide approach[143]. They would welcome a framework which would provide for an alternative to existing formal, as well as informal, channels for cross-border access to electronic evidence while guaranteeing sufficient legal safeguards. If the alternative is introduced, it should not harm the effectiveness of these [currently used] mechanisms that may be slower, but can provide the evidence admissible in courts, according to the respondents.

*Judicial cooperation*

Assertions of extraterritorial jurisdiction could create conflicts of law for foreign providers, unless accompanied by new and sustainable international agreements and approaches,

---

138 Open public consultation feedback: 83.3% (n=36) of respondents from law enforcement and service providers.

139 Open public consultation feedback: 32.9% yes, 45.1% no, 22% no opinion (n=82) of all respondents on question "[…] do you think the possible EU initiative should also cover purely domestic cases?"

140 Open public consultation feedback: 44.44% very relevant, 44.44% relevant, 11.12% no opinion (n=9) of the service providers.

141 Open public consultation feedback: 44.44% yes, 11.12% no, 44.44% no opinion (n=9) of the service providers.

142 Open public consultation feedback: 89% yes, 4% no, 7% no opinion (n=28) of respondents from law enforcement authorities or public authorities directly related to it.

143 Open public consultation feedback: 100% yes (n=20) of respondents from law enforcement authorities or public authorities directly related to it.

according to the respondents. Thus, conclusion of bilateral treaties with the mainly affected countries, such as United States, Russia, Turkey, and Ukraine[144], and conclusion of multilateral treaties enjoyed major support amongst the public survey respondents. Nonetheless, the respondents[145] called for development of an EU-wide common approach to establish an efficient framework which would improve criminal investigations with a non-EU country dimension.

**Service providers** consider sharing information with non-EU countries, in particular with strategic partners such as the United States and Canada, essential. They would welcome process standardisation resulting from an EU-wide common approach and an international framework including bi- and multilateral agreements leading to more time- and cost-efficient information exchange. In any case, the possible international precedents, it might set, and the necessity for sufficient legal safeguards guaranteeing respect to fundamental human rights should be taken into consideration.

Practitioners from **law enforcement authorities** and other public authorities currently experience various difficulties when obtaining evidence with a non-EU country dimension. Most of the practitioners see the lack of a common form as a relevant obstacle[146]; considering an EU-wide approach, a common form would simplify the procedure, and therefore provide for operational savings. Additionally, identification of the responsible counterpart in a non-EU country is also perceived as one of the main difficulties accessing e-evidence with a non-EU country dimension[147].

*Direct cooperation*

Direct cross-border cooperation of law enforcement and judicial authorities with digital service providers would bring added value in criminal investigation according to the vast majority of public consultation respondents[148]. The respondents identified, inter alia, accelerated cost-efficient access to the electronic evidence and legal certainty as the main attributes of such initiative. The majority of respondents[149] would also welcome direct cooperation of EU law enforcement and judicial authorities with digital service providers headquartered in non-EU countries if sufficient safeguards are in place to protect fundamental rights.

144 As identified by the public survey respondents.
145 Open public consultation feedback: 81.7% (n=82) of all respondents selected "very important" or "important".
146 Open public consultation feedback: 22.73% very important, 22.73% important (n=22) of practitioners from law enforcement authorities and public authorities directly related to it.
147 Open public consultation feedback: 40.91% very important, 22.73% important (n=22) of practitioners from law enforcement authorities and public authorities directly related to it.
148 Open public consultation feedback: 73.2% (n=82) of all respondents.
149 Open public consultation feedback: 67.1% (n=82) of all respondents.

The initiative should include a broad range of services in possible direct cross-border cooperation with service providers[150]. Moreover, the respondents called for the broadest possible legal definitions of such services in their comments. As for the two frequently used categories of data, i.e. non-content data and content data, the majority of the public survey respondents supported an EU legal framework for the direct cross-border cooperation with service providers concerning both categories (all types of data) when data is stored in the EU[151]. The data stored outside of the EU should be subject to direct cooperation only when non-content data are concerned, according to slightly more than half of the respondents[152].

Half of respondents supported an EU initiative to enable law enforcement authorities to directly request a service provider in another Member Stated to disclose - on a voluntary basis - specific information about a user without having to go through a law enforcement or judicial authority in the other Member State[153]. A direct cross-border production order which would enable law enforcement authorities to directly compel a service provider in another Member State without having to go through law enforcement or judicial authorities in the other Member State met with somewhat less approval[154]. Concerning non-EU countries, a risk that the initiative would cause a conflict of law and non-EU countries would reciprocally impose similar obligations on the European service providers is a serious concern for many of the survey respondents[155].

A majority of **service providers** believe that direct cross-border cooperation of law enforcement and judicial authorities with digital service providers will bring an added value in criminal investigation[156]. Service providers think an EU initiative could enable law enforcement authorities to directly request a service provider in another Member State to disclose specific information without having to go through a law enforcement or judicial authority in the other Member State[157]. On the other hand, a majority of service providers that responded would not support a direct production order to a service provider in another Member State[158]. Half of the service providers find an increasing volume of requests, which is a considerable driver for costs[159], a very relevant concern[160].

---

150 Open public consultation feedback: 84,15% selected information society service providers, 82,93% electronic communication service providers, and 42,68% other digital services providers in a multiple choice question (n=82).

151 Open public consultation feedback: 69.09% (n=55) of the respondents who answered this question.

152 Open public consultation feedback: 54.24% (n=59) of the respondents who answered this question.

153 Open public consultation feedback: 50% yes, 35.37% no, 14.63% no opinion (n=82).

154 Open public consultation feedback: 43.9% yes, 41.46% no, 14.63% no opinion (n=82) of all respondents.

155 Open public consultation feedback: 66.7% (n=39) of the respondents answering in their personal capacity selected "very relevant" or "relevant".

156 Open public consultation feedback: 60% yes, 10% no, 30% no opinion (n=10) of service providers.

157 Open public consultation feedback: 60% yes, 30% no, 10% no opinion (n=10) of service providers.

158 Open public consultation feedback: 20% yes, 80% no (n=10) of service providers.

159 Open public consultation feedback: 55.56% very relevant, 11.12% relevant, 22.23% somewhat relevant, 11.11% no opinion (n=9) of the service providers.

160 Open public consultation feedback: 55,56% very relevant, 11.12% relevant, 22.23% somewhat relevant, 11.12% not relevant (n=9) of the service providers.

A majority of the practitioners from **law enforcement authorities** and other public authorities would support a possible EU initiative allowing for both a direct production request[161] and a direct production order[162] to a service provider in another Member State. The respondents expect sufficient **safeguards** to be introduced within the limits of the existing framework of the Member States. Furthermore, a non-disclosure clause in the early phases of the criminal investigation would be a necessary measure, which would prevent obstructions in investigations.

The direct production order to the service provider in another Member State, however, did not have much support among the **remaining respondents**[163]. In case the initiative is introduced, it should establish fair, accountable and uniform procedures that govern when and how private companies may be compelled to provide information. Such policies should apply horizontally to all parties that collect and use personal information. In addition, companies should be permitted to challenge in court demands that appear inconsistent.

*Direct access*

Based on the public consultation survey, there is demand[164] for a common EU framework for situations when a law enforcement authority is in possession of a device which provides for access to data relevant to the criminal investigation without any intermediary (e.g. a service provider), although it might be unclear where the data is actually stored or whether there is a cross-border dimension at all. As for the further attributes, respondents mostly agreed that such a proposal should also provide specific safeguards to ensure fundamental rights[165], legal remedies for the person affected (including challenging the admissibility of evidence) [166], notification to another Member Stated affected[167] by this measure and possibility for the notified State to object the measure.

Hampering customer's trust in services is a very relevant concern for a majority of **service providers**[168]. And therefore specific safeguards to ensure fundamental rights[169] and legal remedies for the person affected[170] would need to be introduced if the European Commission should decide to propose a legal framework covering cases with direct access to data without an intermediary. Additionally, the providers expressed their concerns regarding this option as it might, in their opinion, introduce security risks, loss of customer privacy and the confidentiality of communication.

---

161 Open public consultation feedback: 61% yes (n=28) of practitioners from law enforcement authorities and public authorities directly related to it.

162 Open public consultation feedback: 68% yes (n=28) of practitioners from law enforcement authorities and public authorities directly related to it.

163 Open public consultation feedback: 34% yes, 46% no, 20% no opinion (n=44) of citizens and other entities.

164 Open public consultation feedback: 54.9% yes, 24.4% no, 20.7% no opinion (n=82) of all respondents.

165 Open public consultation feedback: 80.49% (n=82) of all respondents.

166 Open public consultation feedback: 80.49% (n=82) of all respondents.

167 Open public consultation feedback: 71.95% (n=82) of all respondents.

168 Open public consultation feedback: 89% very relevant, 11% not relevant (n=9) of the service providers.

169 Open public consultation feedback: 90% yes, 10% no opinion (n=10) of the service providers.

170 Open public consultation feedback: 90% yes, 10% no opinion (n=10) of the service providers.

Practitioners from **law enforcement authorities** and other public authorities would welcome a common EU framework for a situation where direct access to e-evidence through an information system is possible without any intermediary while it is not clear where the data is actually stored or whether there is a cross border dimension at all[171]. In certain Member States, a legal framework covering these cases already exists. According to the respondents, a common EU-wide approach would ensure judicial control and recognition of directly obtained evidence, legal remedies and other safeguards for fundamental rights.

The **remaining respondents** mostly agreed with the need for a framework covering the abovementioned situations[172] although their responses varied with regards to different aspects of such initiative. Possible misuse by authorities is apparently one of the main concerns for the citizens, who often refer to "government hacking". Court supervision and other guarantees should therefore ensure legitimacy and legality[173].

Inception Impact Assessment

The feedback gathered in reaction to the Inception Impact Assessment[174] shows that, in summary, the initiative enjoys significant support as the stakeholders welcome the Commission's efforts to address difficulties public authorities face when obtaining electronic evidence across borders. Addressing the shortcomings of the current MLA system, enhancing effectiveness, improving legal certainty and preventing conflicts of law are seen as the main positive attributes of the proposal. Some concerns regarding various aspects of legal regime and efficiency, however, arise amongst different actors. The business representatives are primarily concerned about any attempt to introduce data localisation requirements as it might have a negative impact on the Digital Single Market and economic diversification. Furthermore, some believe the investigative measures should only concern data from EU subscribers or data stored within the EU.

*Judicial cooperation*

**Business organisations** call for an EU framework allowing for legal cooperation with authorities in non-EU countries to be complemented with durable legal frameworks for international cooperation, so that service providers operating in different jurisdictions are not faced with conflicts of law and conflicting legal obligations, as well as full assessment of the risks arising from reciprocal action of non-EU countries. The US Congress has recently introduced legislation providing for more direct requests to service providers, and the business associations see this as an opportunity to establish a trans-Atlantic cooperation supplementing the current MLA system.

---

171 Open public consultation feedback: 79% yes, 14% no, 7% no opinion (n=28) of practitioners from law enforcement authorities and public authorities directly related to it.

172 Open public consultation feedback: 45% yes, 30% no, 25% no opinion (n=44) of citizens and other entities.

173 Open public consultation feedback: 82% yes, 2% no, 16% no opinion (n=44) of citizens and other entities.

174 Accessible here.

*Direct cooperation*

Direct cooperation with service providers is expected to bring cost savings and efficiency gains for the public sector. Nonetheless, the costs borne by private entities should also be taken into consideration. In particular the costs of establishing a **legal representative** in the EU for SMEs based in non-EU countries were felt to be at risk of being unsustainable. Business representatives are concerned about the proposal to allow EU countries to directly request or compel data from service providers and its possible implications. As it would represent a shift in policy and might trigger a reciprocal reaction from non-EU countries, the private sector calls for a proper impact assessment and clear evidence that the current practice is not sufficient.

*Direct access*

The legislative option to access e-evidence without cooperation of a service provider would require judicial oversight with sufficient safeguards to ensure protection of fundamental rights. It could be limited to emergency cases, according to the stakeholders who fear this practice would lead to an erosion of trust amongst citizens.

Targeted survey 1

The replies to the targeted survey 1 revealed that there is **no common approach** to obtain cross-border access to digital evidence, for which each Member State has developed its own domestic practice. There is a large variety of approaches adopted by the Member States and their law enforcement and judicial authorities as well as by the service providers. This diversity, which seems mainly due to the lack of a legal framework and of a common approach on how to access e-evidence and deal with requests to share information, creates **legal uncertainty** for all the stakeholders involved and represents an obstacle to joint and cross border investigations.

*Judicial cooperation*

The feedback gathered focused on the judicial cooperation between public authorities in the Member States and non-EU countries:

- Mutual Legal Assistance (MLA) is in this area mainly based on **international law**, notably the Council of Europe Budapest Convention on Cybercrime. Besides that, there are agreements concluded by the EU (notably, the Agreement on MLA between the EU and the U.S.) and several **bilateral agreements**, which most Member States have concluded with the US, followed by Canada and Australia.
- The systematic use of MLA for all types of access requests for electronic evidence is increasingly viewed as **problematic** as the requests take too long to be processed (a minimum of 1 month to a maximum of 18 months), there are no fixed deadlines for responding, and the mechanism is complex and diverges from country to country (i.e. in most of the countries the formal procedure for issuing an MLA is initiated by prosecutor, followed by judge, law enforcement, diplomatic channel or central authorities).

- When it comes to cooperation with the US in particular, challenges identified concern the use of MLA procedures for access to information where under U.S. law no MLA request is required, such as for subscriber or traffic data. MLA requests for such information significantly increase the overall volume of requests and contribute to **slowing down** the system. The use of MLA for such requests can be attributed to various reasons, including (1) where the issuing of a direct request is not permitted under the law of the issuing country; (2) where enforceability of the request is desired; and (3) a lack of awareness of the issuing authority about alternative channels.
- The **admissibility of MLA requests** is subject to the receiving countries' legal system, which may result in a refusal of the MLA request (most Member States indicated as ground for refusal the difficulty to establish probable cause, followed by the lack of dual criminality, data not available due to deletion, incomplete or inadequate requests).
- MLA is often used to obtain **access to content data** (22 Member States), but it is also used to obtain other types of information, including **subscriber** and **traffic data**. "Top" non-EU countries to which most Member States send the requests are the US and Canada.
- Although MLA requests are made following formal channels, it is difficult to keep track of both requests and responses to non-EU countries with the effect that most Member States do not have available **statistics for e-evidence**.
- The **means of transmission** are generally **inadequate** as most of the Member States make use of letter, fax or email, with very few countries using secure channels.
- These formal procedures ensure that the right authorities are involved and that appropriate **safeguards** are taken into account when there is a sovereign interest of more than one country. They also have the consequence that requests for mutual legal assistance require considerable time to be processed, even in cases with little or no connection to the receiving country besides the seat of the service provider.
- The legal framework is **fragmented** and complex; practitioners are faced with a high number of bi-lateral and multi-lateral conventions and with the specific requirements of recipient countries' legal systems. For example, for requests addressed to the U.S., the probable cause requirement has to be met to allow the disclosure of content data, which is a concept foreign to EU practitioners, who sometimes struggle with it.
- The EU-U.S. MLA Review Report of 2016 underlines that delays are due to **bottlenecks** at the phase of the reception of requests by the U.S. Authorities and also during the execution phase. This is mainly due to the steep and sustained increase in volume of requests; as the U.S. authorities reported already in 2014, "[o]ver the past decade the number of requests for assistance from foreign authorities handled by the Criminal Division's Office of International Affairs (OIA) has increased nearly 60 percent, and the number of requests for computer records has increased ten-fold." In an effort to improve the situation, the U.S. Department of Justice has created a dedicated team for electronic evidence and has obtained a change in legislation allowing them to make the relevant pleas before the local District of Columbia courts. Nonetheless, the resources continue to be outmatched by the swift growth in requests.

*Direct cooperation*

- EU Member States and their judicial and law enforcement authorities have taken diverging approaches as regards the use of the connecting factors for the exercise of an investigatory measure allowing for access to e-evidence. There are different ways of determining whether a provider is to be considered domestic or foreign and the criteria to distinguish between domestic and foreign service providers vary significantly among the Member States, ranging from the "main seat of the service provider" (16 Member States) and "the place where services are offered" (6 Member States) to "the place where data is stored" (6 Member States) and a combination of alternatives.
- Moreover, while 14 Member States consider direct requests sent from national authorities directly to a service provider in another country as **voluntary** for the provider to comply with, 7 Member States consider these requests as **mandatory**. Even when this mechanism is considered mandatory, it is very difficult to assess whether the Member States can actually enforce it, also due to the lack of a specific legal framework for these requests (20 Member States apply to these cases the same framework as for domestic requests) or agreement with foreign service providers (only 8 Member States have such agreements).
- The majority of national legislations either **does not cover or explicitly prohibit** that service providers established in the Member State **respond to direct requests** from law enforcement authorities from another EU Member State or non-EU country[175].
- The **definition of types of data** (subscriber, traffic and content data) varies significantly among Member States, while specific categories of data exist in several countries. **Data requested** from service providers are generally subscriber (21 Member States) and traffic data (18 Member States), while in a few Member States (9) it is also possible to request content data and "other data" (4 Member States).
- Practices also diverge as regards the **procedures for making the direct requests**, i.e. the authority which can initiate the process (generally the police, followed by the prosecutor and the judge), the modality for launching a request or transmitting e-evidence (normally via email or web portal, but in some other cases with paper or fax or via all the possible means). The only common feature is the lack of a central repository in the Member States.
- There is no common approach on how the service providers react to requests from foreign law enforcement authorities and it appears they respond differently depending on which country requests come from, with a minimum **responding time** of a few minutes in certain countries to a maximum of 1 month in others.
- **Admissibility in Court** of e-evidence gathered outside the MLA mechanism does not generally constitute a problem for the majority of Member States, with the exception of a few Member States where this is not allowed by domestic laws or it is subject to

[175] As regards non-EU countries, the General Data Protection Regulation (Regulation (EU) 2016/679) and the Directive on data protection in the police and criminal justice field (Directive (EU) 2016/681) applicable from May 2018 set certain requirements on transfers of personal data in this context.

stringent conditions, showing the lack of a common view on the principle of voluntary disclosure without an MLA among Member States.

*Direct access*

- In some Member States, law enforcement authorities make use of investigative techniques to access e-evidence also when **the location of e-evidence is unclear** or **impossible to establish**. Tools used across the EU range from "remote access" and "search and seizure" to "multiple MLA requests" and "instruments of international cooperation". On the other hand, there are still several countries (8 Member States) where the access to e-evidence under these circumstances is not possible or provided for by law.

Targeted survey 2

- The targeted survey revealed that:
  - **More than half** of total investigations include a request to **cross-border access to e-evidence**.
  - **Less than half of all the requests to service providers are fulfilled.**
  - Almost **two thirds** of crimes involving cross-border access to e-evidence **cannot be effectively investigated or prosecuted.**
- The survey was based on **estimates** since this data is not collected in Member States.
- The results of the survey have been integrated in section 2.1.1 of the impact assessment (Definition and magnitude of the problem).
- For more details, please see Annex 11 (Additional data on the size of the problem).

Targeted survey 3

- This survey provided input that was used to estimate the costs and benefits that the different options would generate for **Member States**.
- See section 6.2. (Quantitative assessment) and Annex 3 for a summary of the costs and benefits and Annex 4 for a detailed description on the model to estimate those costs and benefits.

Targeted survey 4

- This survey provided input that was used to estimate the costs and benefits that the different options would generate for **service providers.**
- See section 6.2. (Quantitative assessment) and Annex 3 for a summary of the costs and benefits and Annex 4 for a detailed description on the model to estimate those costs and benefits.

See Annex 2.1. for procedural information on all the surveys carried out.

## 2. Meetings

The meetings, and in particular the "expert process" organised by the Commission, were an integral part of the consultation activities and were instrumental in developing the problem definition and the options described in the impact assessment.

As indicated below, the feedback was taken into account and regularly summarised into documents that the Commission made public in the **website of this initiative**[176].

The feedback received in the meetings was not limited to ideas presented by the Commission. In many occasions, they were the stakeholders themselves who produced ideas for discussion. For example:

- Concerning **direct cooperation**, Belgium presented a similar model to the EPO, i.e. an obligation for companies which provide a service on EU territory (the so-called business link) to comply with EU rules and to execute national orders to provide communication data when such orders are issued by a competent authority of an EU Member State. This obligation should be enforced by a sanctions regime. It includes a possible obligation for the investigating country to demand prior or posterior agreement by other affected countries, supported by a clear definition of cases in which another country is affected by the request. BE proposed to combine two parameters: the sensitivity of the measure and the location of the target. BE considered that for the less sensitive production orders, e.g. for subscriber data, there is no need to notify another country. For more sensitive measures, such as an order to produce content data, the key factor should be where the intrusion on the privacy of the target takes place.
- Concerning **direct access**, Germany submitted a proposal based on a system of notification/validation similar to Art. 31 EIO Directive. The criterion to determine the State affected by the investigative measures could be firstly the Member State of storage. If the investigating Member State is unable to identify the Member State of storage swiftly and with a reasonable amount of effort, the Member State of habitual residence of the person who regularly utilises the data affected by the investigative shall be informed.

See Annex 2.2. for procedural information on the different meetings in which feedback from stakeholders was gathered.

## 3. Conferences

The conferences were an opportunity to present the Commission's work and gather feedback in person from stakeholders in a setting that allows a wider reach than the above meetings.

[176] See here.

The input received in the conferences, shaped the ongoing work of the Commission and was incorporated in the meeting discussions, fed into the survey questions and added to the relevant sections of the impact assessment.

See Annex 2.2. for procedural information on the different conferences in which feedback from stakeholders was gathered.

**3) How the results have been taken into account**

The results of the consultation activities have been incorporated throughout the impact assessment in each of the sections in which feedback was received.

The consultation activities were designed to follow the same **logical sequence** as the impact assessment, starting with the problem definition and then moving on to possible options and their impacts.

This logical sequence can be observed in the documents that the Commission has been publishing in the **more than 1.5 years** of consultation activities for this initiative, and which provided **regular updates** on the progress of the Commission work with the different stakeholders. The documents containing these regular updates were **made public** as soon as they were ready and published in the **Commission website** of this initiative.

Using the same logical sequence in the consultation activities as in the impact assessment facilitated the incorporation of the stakeholders' feedback into the different sections of the impact assessment.

This impact assessment is therefore built on the input of a large number of consultation activities in multiple forms and with a wide range of stakeholders, to whom the Commission is grateful for their **fundamental** contributions.

## Annex 2.1: surveys

### 1) Open public consultation

The European Commission launched an open public consultation[177] on 4 August 2017 which closed after 12 weeks, on 27 October 2017.

It aimed to gather feedback on current practices on obtaining cross-border electronic evidence in the Member States as well as on practical and legal problems arising both at national and EU level from gaps and weaknesses of existing regulations. It also listed possible options to address shortcomings and provided an opportunity to indicate preferences for elements that should be included in a solution. It was addressed to a broad range of interested stakeholders, including public authorities, judges, prosecutors, EU institutions and agencies, international organisations, private companies, professional and business associations, NGOs, academics and the general public

The Open Public Consultation was conducted through an online questionnaire published on the internet in all EU official languages, with the exception of Gaelic. It was advertised on the European Commission's website, through social media channels (DG HOME and Europol's EC3 Twitter accounts), through established networks of stakeholders (e.g. contacts held by the European Cybercrime Centre at Europol) and at all relevant meetings.

82 responses were collected: 22 from individuals in the general public and 60 from practitioners in a professional capacity or on behalf of an organisation.

Among the 22 responders from general public, there were 13 persons who are affected by legislation in this area as citizens or users of digital services, 3 as lawyers, 1 as an academic, 1 as an employee of an NGO, and 4 as public servants or staff of a criminal justice authority. The members of the general public selected a range of countries of residence: AT, BE, DE, ES, FR, IT, LX, PT, RO, SW, UK and US.

29 practitioners were members of law enforcement or judicial authority or public authority directly related to it (e.g. Ministry of Justice, Ministry of Interior), which is the largest professional group among the 60 practitioners who submitted the questionnaire in their professional capacity or on behalf of an organisation. Other responders included:

- private companies (private sector);
- trade, business or professional associations (e.g. national banking federations);
- non-governmental organisations, platforms or networks;

[177] Available here.

- professional consultancies, law firms, self-employed consultants;

They were based across 17 European countries (AT, BE, CZ, DE, EE, ES, FI, IE, IT, LV, NL, PT, RO, SK, SL, SW, UK), Norway and US.

The respondents could also upload a document in order to provide additional information or raise specific points which were not covered by the questionnaire. The following entities submitted additional information:

- Access Now, Belgium.
- American Chamber of Commerce to the EU (AmCham EU), Belgium
- Bayerisches Staatsministerium der Justiz, Germany
- BSA | The Software Alliance, Belgium
- Center for Democracy and Technology, United States of America
- CISPE (Cloud Infrastructure Service Providers in Europe), Belgium
- Cloudflare, United States of America
- Council of Bars and Law Societies of Europe (CCBE), Belgium
- Dataskydd.net Sverige, Sweden
- Deutscher Richterbund, Germany
- DIGITALEUROPE, Belgium
- Dutch National Public Prosecutor's Office, Netherlands
- eco - Verband der Internetwirtschaft e.V., Germany
- ETNO - European Telecommunications Network Operators' Association, Belgium
- EuroISPA, Belgium
- European Digital Rights (EDRi), Belgium
- Global Network Initiative, United States of America
- Privacy International, United Kingdom
- Telenor Group, Norway
- Vodafone Group plc

The responses to the public consultation that agreed to be published are available in the dedicated consultation webpage[178].

Inception Impact Assessment:

The Open Public Consultation contained a link to the Inception Impact Assessment, which the Commission published at the same time as the Open Public Consultation.

[178] See here.

In total, 10 comments were submitted: 2 by EU citizens, 2 by academia/research institutions, 3 by business associations, and 3 by business entities.

Interested stakeholders could provide feedback to the Inception Impact Assessment from 4 to 31 August 2017.

**2) Targeted surveys**

Targeted survey 1

The purpose of this survey was to gather information on the current **state of play** in Member States concerning cross-border access to e-evidence. In particular, it addressed the **current practices** in the Member States concerning 1) direct cooperation between law enforcement authorities and private sector service providers, 2) mutual legal assistance or mutual recognition procedures and 3) enforcement of jurisdiction in cyberspace, namely other measures that law enforcement authorities could use to obtain e-evidence in cases when it is not clear they would operate within their own jurisdiction. The questionnaire was developed taking into account previous and ongoing activities, including the GENVAL evaluation, and sought to complete the picture.

The survey was addressed to public authorities in all Member States.

The Commission received replies from 25 Member States (all except BG, LU and PL). The national replies were coordinated at national level amongst different responsible ministries, the judiciary and law enforcement authorities.

The questionnaire was launched on 29 July 2016 and closed on 16 September 2016, although the last responses from Member States were received on 28 February 2017.

Targeted survey 2

The purpose of this survey was to collect quantitative and qualitative information on the **size of the problem** concerning cross-border access to e-evidence through both judicial cooperation channels and direct cooperation between public authorities and service providers.

The survey was addressed to public authorities in all Member States.

In total, 76 responses were received through the online survey from public authorities from all Member States except EL and PL. SE sent the information by email. 68 responses came from law enforcement, 5 from judicial authorities, and 4 from the public administration officials.

The survey was sent on 6 October 2017 and it was closed on 23 October 2017.

Targeted survey 3

The purpose of this survey was to collect information on the **costs and benefits** (e.g. cost savings) that the different options would generate **for Member States**.

The online survey was sent to public authorities in all Member States, including state police departments, national cybersecurity units, state prosecutors offices, ministries of justice, and ministries of interior. The survey included 26 questions, both open- and closed-ended.

A total of 13 responses from authorities representing 11 Member States were received.

The survey was sent on 25 October 2017 and it was closed on 8 November 2017.

Targeted survey 4

The purpose of this survey was to collect information on the **costs and benefits** that the different options would generate **for service providers**.

The online survey was sent to 17 major service providers legally established within and outside the territory of the EU and 3 business associations. The survey included 13 questions, both open- and closed-ended.

A total of 10 responses were received from service providers covering internet infrastructure services, telecommunications services, electronic communications services, cloud services, hosting services, and digital forensics services.

The survey was sent on 25 October 2017 and it was closed on 8 November 2017.

## Annex 2.2: meetings

To define and scope the problems, to map different initiatives, to draw up possible options and identify impacts, the Commission services organised and participated in various group meetings: with Member States, including the Presidency, with other stakeholders, including the Council of Europe, Interpol, UNODC, the European Judicial Network but also with a number of private sector service providers and civil society organisations.

Group expert meetings

- On 12 July 2016, an experts' meeting with **academics and practitioners from Member States** took place covering the relationship between different channels for obtaining cross-border access to electronic evidence, including direct cooperation and Mutual Legal Assistance, as well as the concepts of establishing investigative jurisdiction and enforcing jurisdiction.
- On 15 September 2016, in conjunction with the **EU Internet Forum**, the Commission services held a workshop with service providers (including Microsoft Google, Apple, Twitter and Facebook representatives) and members and representatives of industry associations (CCIA, BSA and DIGITALEUROPE) that issued a supporting statement[179], with the objective to compare assessments of the current status quo and exchange views.
- On 4 October 2016, an experts' meeting with **Member State practitioners, European Judicial Network (EJN) and Eurojust** representatives discussed the use of **Mutual Legal Assistance within the Union**, notably the possible use of the European Investigation Order (EIO) for cross-border access to electronic evidence and in particular its annex A with regard to its suitability for requesting access to digital evidence, as well as the possible requirements for an IT portal to exchange requests.
- On 4 October 2016, the Commission intervened at a meeting of the **European Chiefs of Cybercrime Units (EUCTF)** to provide an update on the work on cross-border access to electronic evidence. The discussion focused on challenges that national units face in making direct requests to providers established in another country (e.g. the U.S.) for basic subscriber information or traffic data/metadata.
- On 9 November 2016, an expert meeting with representatives of **Member States, the EJN, Eurojust and the Council** secretariat, and technical experts working on e-codex MLA, Interpol and Evidence projects discussed the way forward towards "a secure online portal" for requests and responses concerning e-evidence.

[179] Joint statement of The Computer & Communications Industry Association (CCIA Europe), BSA │The Software Alliance, and DIGITALEUROPE of 10 June 2016 on the 9 June 2016 Conclusions of the Council of the European Union on improving criminal justice in cyberspace.

- On 17 and 18 January 2017, an expert meeting was organised with representatives of all **Member States** (except for Greece), from **Europol, the Council General Secretariat, the European Parliament LIBE Secretariat, the Counter-Terrorism Coordinator's office, an independent expert** and the Commission task force on e-evidence. The expert meeting served to discuss the current legislative framework and use of domestic production orders and other investigatory measures, notably direct access through a computer system.
- On 28 February 2017, an expert meeting was organised with representatives of all **Member States, from Europol, the Council General Secretariat, the LIBE Secretariat, the Counter-Terrorism Coordinator's office**, an independent expert and the Commission task force on e-evidence. The expert meeting discussed **practical measures** for improving direct cooperation between law enforcement authorities and private sector service providers, notably when service providers are located in another country.
- On 6 March 2017 a roundtable meeting with **service providers, industry associations and civil society organisations** was held in connection with the EU Internet Forum. The Commission presented the state-of-play and answered several questions on e.g. the scope of the work and policy options considered.
- On 3 and 4 April 2017, an expert meeting was organised with representatives of all **Member States** (except Greece), **Europol, Eurojust**, a number of members of the **Council of Europe T-CY Bureau**, members of the **Council General Secretariat, the LIBE secretariat and an independent expert** supporting the Commission. The expert meeting discussed possible avenues for **reforming the current legal framework**, notably on options as regards the types of e-evidence, direct cooperation and direct access.
- On 26 and 27 April 2017, an expert meeting was organised with representatives of all **Member States** (except Greece and Malta), from **Europol, the Council General Secretariat and the Counter-Terrorism Coordinator's office.** The expert meeting continued the discussions on possible avenues for **reforming the current legal framework**, notably on options as regards the types of e-evidence, direct access and user notification.
- On 2 May 2017, under the auspices of the EU Internet Forum a targeted roundtable meeting was held with **service providers, industry associations and civil society** organisations in order to obtain targeted feedback on **user notification** and **costs** involved with requests for cross-border access to electronic evidence.
- On 10 May 2017, under the auspices of the EU Internet Forum, a targeted roundtable meeting was held with **service providers, industry associations** and **civil society** organisations on e-evidence in order to obtain targeted feedback on **connecting factors for the use of investigative measures** and **conflicts of law**.
- On 15 September 2017, an expert meeting was organised with representatives of all **Member States, the Council General Secretariat and the Counter-Terrorism**

**Coordinator's office**. The expert meeting continued the discussions on possible avenues for **reforming the current legal framework**, notably on the different options for two possible legislative measures: **production order/production request and direct access**, including a draft work plan for practical measures on direct cooperation with service providers.

- On 2 October 2017, an expert meeting on data protection aspects of cross-border access to electronic evidence was organised with representatives of **Member States** (except EL, PT, CY, DK, CZ, HR, LV), **data protection authorities** (from BE, BG, CZ, FR, IE, LU, LV, PL, SI, SK), including the **EDPS.** The meeting focused on different aspects of the **production order/request**, notably the personal, material and geographical scope of the measure, user notification, as well as the appropriate legal basis for **direct access**.
- On 18 October 2017, an expert meeting was organised with representatives of all **Member States** (except Greece and Cyprus) and **the Counter-Terrorism Coordinator's office**. The expert meeting continued the discussions on possible avenues for **reforming the current legal framework**, notably on the following aspects of the **production order**: legal representative, enforcement, safeguards, legal remedies, and personal scope.

Bilateral meetings

The list below contains the bilateral meetings in which the Commission participated to gather feedback from stakeholders. It includes bilateral meetings with:

- Service providers, including individual companies and industry associations, focused on direct cooperation.
- Public authorities from Member States, including the liaison magistrates from Member States in the US.
- Europol.
- US public authorities (Department of Justice), in various forms:
    - Regular videoconferences;
    - EU-US Ministerial Meeting;
    - Meeting in person at working level through a fact-finding mission to the US.

  The discussions focused on judicial cooperation.
- Academia, covering judicial cooperation, direct cooperation and direct access.
- NGOs.

Bilateral meetings included:

| | |
|---|---|
| 14 Apr 16 | Microsoft |
| 31 May 16 | Apple |
| 17 Jun 16 | Eurojust |
| 19 July 16 | Slovakian Presidency |
| 30 Jun 16 | Belgium – Ministry of Justice |
| 28 Jul 16 | Apple |
| 29 Jul 16 | US Department of Justice |
| 01 Aug 16 | Google |
| 09 Aug 16 | Twitter |
| 10 Aug 16 | Facebook |
| 22 Aug 16 | Microsoft |
| 14 Sep 16 | Center for Democracy and Transparency (CDT) |
| 14 Sep 16 | BSA \| The Software Alliance |
| 27 Sep 16 | German JHA Counsellor |
| 27 Sep 16 | Hessen Minister of Justice |
| 28 Sep 16 | Estonia JHA Counsellor |
| 13 Oct 16 | Estonian Minister of Justice |
| 18 Oct 16 | Maltese Presidency |
| 24 Oct 16 | Slovakia Presidency |
| 04 Nov 16 | Maltese Presidency preparation delegation |
| 09 Nov 16 | Facebook |
| 10 Nov 16 | Council of Europe |
| 01 Dec 16 | Estonian Perm Rep |
| 05 Dec 16 | EU-US Ministerial Meeting |

| | |
|---|---|
| 07 Dec 16 | BSA \| The Software Alliance |
| 08 Dec 16 | Google |
| 19 Dec 16 | Professors Frank Verbruggen and Vanessa Franssen in presence of Mr. Francois Falletti, former Prosecutor General |
| 22 Dec 16 | Prof Vanessa Franssen |
| 23 Dec 16 | Maltese Presidency |
| 13 Jan 17 | UK Perm Rep |
| 16 Jan 17 | Austrian Minister of Justice |
| 26 Jan 17 | Apple |
| 27 Jan 17 | Google |
| 27 Jan 17 | Prof. Jennifer Daskal, American University |
| 31 Jan 16 | Twitter |
| 01 Feb 16 | Council Counter-Terrorism Coordinator staff |
| 01 Feb 17 | LIBE secretariat |
| 03 Feb 17 | Symantec Corporation |
| 07 Feb 17 | Discussion with Prof. Falletti |
| 08 Feb 17 | Discussion with cabinet of Minister Koen Geens |
| 08 Feb 17 | Eurojust |
| 09 Feb 17 | Videoconference with EUDEL USA - Liaison Magistrates |
| 09 Feb 17 | US Department of Justice |
| 01 Feb 17 | EuroISPA (European Internet Services Providers Association) |
| 01 Feb 17 | LIBE Secretariat |
| 23 Feb 17 | Facebook |
| 27 Feb 17 | Belgium - Ministry of Justice |
| 03 Mar 17 | EVIDENCE project videoconference |
| 07 Mar 17 | Microsoft |

| | |
|---|---|
| 07 Mar 17 | US Department of Justice |
| 11 May 17 | Minister of Justice of Belgium |
| 22 Mar 17 | Minister of Justice of Romania |
| 24 May 17 | Minister of Justice of Greece |
| 24 Mar 17 | LIBE Secretariat |
| 27 Mar 17 | CDT |
| 03 Apr 17 | Netherlands Ministry of Justice |
| 10 Apr 17 | Cabinet of BE Minister of Justice |
| 10 Apr 17 | Professor Ligeti |
| 19 Apr 17 | Microsoft |
| 26 Apr 17 | Deputy Assistant Attorney General Richard Downing, as part of US dialogue |
| 05 Apr 17 | Minister of Justice of Ireland |
| 02 May 17 | Council of Europe – T-CY secretariat |
| 30 May 16 | Professor Ligeti and Microsoft |
| 01 Jun 17 | US Department of Justice |
| 07 Jun 17 | French Minister of Justice |
| 09 Jun 17 | US Department of Justice |
| 13 Jun 17 | European Data Protection Supervisor |
| 20 Jun 17 | Professor Ligeti |
| 20 Jun 17 | EuroISPA |
| 20 Jun 17 | Facebook |
| 20 Jun 17 | Symantec |
| 20 Jun 17 | Twitter |
| 20 Jun 17 | Google |
| 28 Jun 17 | US House of Representatives |

| | |
|---|---|
| 10 Jul 17 | German Ministry of Justice |
| 03 Jul 16 | Professor Ligeti |
| 17 Jul 17 | Estonian Permanent Representation, EU-US JHA Council prep meeting |
| 20 Jul 17 | Discussion with Prof. Sieber and Prof. Ligeti |
| 24 Jul 17 | Update to Member States at HWP Cyber Issues |
| 27/28 Jul 17 | Experts from the Bavarian Police and the Bavarian Central Office for the Prosecution of Cybercrime |
| 04 Sep 17 | US Department of Justice |
| 06 Sep 17 | Symantec |
| 07 Sep 17 | Belgium – Ministry of Justice |
| 25 Sep 17 | Facebook |
| 26 Sep 17 | Spanish Permanent Representation |
| 29 Sep 17 | Professor Ligeti |
| 04 Oct 17 | La Commission Nationale de l'Informatique et des Libertés (CNIL) |
| 09 Oct 17 | UK Permanent Representation and Home Office |
| 11 Oct 17 | Belgium – Ministry of Justice |
| 13 Oct 17 | Europol Sirius Project |
| 17 Oct 17 | Czech Confederation of Industry |
| 17 Oct 17 | The German Marshall Fund with US Members of Congress |
| 19 Oct 17 | Electronic Frontier Foundation and EDRi |
| 23 Oct 17 | Microsoft |
| 24 Oct 17 | European Data Protection Supervisor |
| 12 Oct 17 | Czech Government Co-ordinator of Digital Agenda |
| 23 Oct 17 | Microsoft |
| 13 Nov 17 | French Minister of Justice |
| 17 Nov 17 | Microsoft |

| | |
|---|---|
| 20 Nov 17 | Meeting with Member States' experts to validate assumptions for quantitative and qualitative analysis |
| 20 Nov 17 | Meeting with service providers to validate assumptions for quantitative and qualitative analysis |

## Annex 2.3: conferences

Commission representatives also participated in various workshops and conferences to and gather additional input.

The list below contains the conferences and workshops organised by third parties in which the Commission participated to provide information on the ongoing work and gather feedback from stakeholders. It includes conferences with bilateral meetings organised by:

- NGOs.
- Public authorities from Member States.
- Intergovernmental organisations.

The discussions addressed judicial cooperation, direct cooperation and direct access.

List of conferences:

| | |
|---|---|
| 08 Sep 16 | DIGITALEUROPE |
| 27 Sept 16 | Panel on cybercrime organised by the Permanent Representation of Hessen |
| 19 Oct 16 | SENTER conference, Vilnius |
| 14 Nov 16 | Internet and Jurisdiction conference, Paris |
| 17 Nov 16 | Forum Europe 4th Annual European Cybersecurity Conference |
| 23 Nov 16 | CEPS EUnited against crime: digital evidence, privacy and security in the EU |
| 25 Jan 17 | Computers, Privacy and Data Protection (CPDP) Conference Panel on Privacy and Cross-Border Requests for Data |
| 26 Jan 17 | Digital Privacy and Security Working Group |
| 27 Feb 17 | Internet&Jurisdiction project call |
| 25 Apr 17 | Law enforcement challenges in the online context, University of Luxembourg |
| 02 May 17 | Council of Europe Budapest Convention Committee |
| 04 May 17 | ALDE Digital Working Group |
| 12 May 17 | Council Horizontal Working Party on Cyber Issues |

| | |
|---|---|
| 19 May 17 | EuroDIG Panel on Criminal Justice on the Internet: Identifying common solutions |
| 31 May 17 | Internet&Jurisdiction Project call |
| 1 June 17 | CDT Digital Security/Privacy WG Call on Developments in the EU and US on Cross Border Law Enforcement Demands |
| 7-9 June 17 | Plenary meeting of the Convention Committee (T-CY) of the Council of Europe Budapest Convention on Cybercrime |
| 20 Jun 17 | Internet&Jurisdiction Project call |
| 27 Jun 17 | Digital Advisory Council |
| 24 Jul 17 | Internet&Jurisdiction Project call |
| 19 Sep 17 | BITKOM Privacy Conference: Panel on “Law Enforcement and Multilateral Legal Assistance Treaties” |
| 09 Nov 17 | Panel on "Finding Solutions for Law Enforcement Access to Digital Evidence" |
| 16 Nov 17 | EURACTIV & Microsoft panel debate "Digital Evidence: Europe’s Fragmented Crime Scene" |

**ANNEX 3: WHO IS AFFECTED AND HOW?**

## 1. Practical implications of the initiative

*For individuals*

The initiative primarily addresses Member States' law enforcement and judicial authorities and digital service providers (businesses) that are active on the EU market. The initiative does not contain regulatory obligations for citizens and/or consumers, thus, does not create additional costs related thereto.

*For digital service providers (businesses)*

The practical implications of this initiative are related to two areas: non-legislative action and the direct cooperation legislation.

As for the non-legislative actions, the measures proposed would be voluntary and thus compliance will depend on the willingness of the service providers to take these actions. The main implications will be the creation of the SPOC and streamlining service providers' policies. Implementation of these measures is expected to take place in 2018-2019.

Those practical measures addressed to service providers (single points of entry, streamlining of policies) would generate some costs for service providers, in particular if changes to procedures and standard terms of contracts have to be implemented, but public authorities would be faced with less, more consistent requests and policies, and would not have to adapt to a variety of individual service providers' policies, leading to cost reductions for them.

The key obligations would result from the direct cooperation legislation which would require service providers providing data directly to public authorities in other Member States. As explained in Annex 4, for both the public and the private sector, administrative and compliance costs arise from implementing new legislation. Service providers would also have to adapt their standard terms and conditions to the new legal framework. A moderate increase in the total number of requests being issued by public authorities could be expected.

A cost-generating factor for the service providers would be the obligation to designate a legal representative in the Union, in particular for service providers not established in the Union, who would have to mandate somebody in the Union to carry out this task. In particular for SME's, there is a fear that this could represent an important burden. On the other hand, this legal representative could be shared between service providers, and the legal representative may accumulate different functions (e.g. GDPR or ePrivacy representatives in addition to the production order legal representative). In addition, they

would have to establish internal procedures so that the legal representative, upon request, gets the data concerned within the deadline.

A combination of 7 measures would result in cumulated cost reductions for the service providers compared to the baseline scenario.

*For Member States, law enforcement and judicial authorities*

Same as for the service providers, the measures proposed under non-legislative actions, would be voluntary and thus compliance will depend on the willingness of the Member States to take these actions. The main implications will be the development of the secure online platform, the creation of the SPOC and of an online portal, standardisation and reduction of forms used by law enforcement and judiciary, and training. Implementation of these measures is expected to take place in 2018-2019.

The development of the secure online platform and the implementation of practical measures to improve cooperation between public authorities and service providers, in particular those that are addressed to public authorities (SPOC, training, standardised forms, online portal) would generate some costs for public authorities,[180] as explained in Annex 4 to this impact assessment. At the same time, they would also improve the quality of requests and would therefore lead to an overall reduction of resources and costs for both service providers and public authorities.

The public sector would incur administrative and compliance costs from implementing new legislation on direct cooperation, as explained in Annex 4.

Same as for the service providers, the combination of 7 measures would result in cumulated cost reductions for the public authorities compared to the baseline scenario. The expected shift from judicial cooperation channels to cooperation with service providers would lead to important cost savings to law enforcement and judicial authorities (administrations) by eliminating administrative tasks related to issuing and recognising requests for data to other authorities. A summary of the changes to administrative procedures as compared to the existing system are illustrated in the following tables:

[180] The costs would depend on how Member States would implement this measure.

| | Today | Under the proposed new initiative |
|---|---|---|
| Terrorism investigation: request for production of content data to IE using **MLA** (see section 2.1.2.) | **MLA**:<br>1. National request prepared and judicially approved based on individual national standard<br>2. Submitted to central authority for review<br>3. Sent from central authority to central authority<br>4. Assessed by receiving central authority and assigned<br>5. Transformed into national order<br>6. Served on service provider<br>7. Service provider responds to executing national authority if possible<br>8. Executing national authority sends to requesting national authority<br>9. Requesting national authority sends to requesting judicial authority<br>10. Content data introduced as evidence in court; admissibility verified | **European Production Order:**<br>1. National request prepared and judicially approved based on harmonised EU standard and its conditions<br>2. served on service provider<br>3. Service provider responds within deadlines if possible (data available, no conflicting obligations)<br>4. Produced data introduced as evidence in court; admissibility verified<br><u>Advantages:</u><br>• Reduction of administrative burden for cases in which the receiving authority typically has no own interest because there is<br>o No connection between the location of service provider establishment and the case (e.g. Facebook in US holding data on German citizen suspected in German case)<br>o No connection between the data storage location and the case<br>o No connection between the location of the user concerned and the establishment of the service provider |
| Child sexual abuse: request for production of access log data to US-based service provider using **voluntary direct cooperation** (see section 2.1.2.) | **Voluntary direct cooperation**:<br>1. National request prepared and judicially approved based on individual national standard<br>2. Sent to service provider<br>3. Service provider reviews based on its individual policy | |

| | Today | Under the proposed new initiative |
|---|---|---|
| | 4. Service provider takes a voluntary decision to provide information<br><br>5. Data introduced as evidence in court; admissibility verified | ○ Low impact on fundamental rights<br><br>• Increased speed which is essential as data swiftly disappears<br><br>• Legal certainty for authorities and service providers, some of whom already provide information based on 28 different requests and subject to their own individual specifications<br><br>• Increased transparency on conditions and process<br><br>• Ideal scenario: central IT system to channel requests<br><br>○ would facilitate accountability and audits<br><br>○ would permit reliable authentication<br><br>○ would reduce burden on smaller providers<br><br>○ could allow for connection with automated national and company solutions where those are available |
| Human trafficking: request for **direct access** (see section 2.1.2.) | **Direct access**: National request prepared and judicially approved based on individual national standard; judicial approval subject to national criteria on location of data; may be refused | **Direct access:** National request prepared and judicially approved based on harmonised standard and agreed connecting factors ensuring greater respect for comity; possible notification to relevant other countries |

| | Today | Under the proposed new initiative |
|---|---|---|
| Cybercrime: search of Domain Name **WHOIS system** (see section 2.1.2.) | **WHOIS Database** lookup performed based on general competence to search publicly available data | **WHOIS Database** lookup performed based on general competence to search specific types of non-public data made available for law enforcement |
| Typical use case 1: production of subscriber information, using **MLA** | **MLA**:<br>1. National request prepared and judicially approved based on individual national standard<br>2. submitted to central authority for review<br>3. sent from central authority to central authority<br>4. Assessed by receiving central authority and assigned<br>5. transformed into national order<br>6. served on service provider<br>7. Service provider responds to executing national authority if possible<br>8. Executing national authority sends to requesting national authority<br>9. Requesting national authority sends to requesting judicial authority<br>10. Data introduced as evidence in court; admissibility verified | **European Production Order:**<br>1. National request prepared and judicially approved based on harmonised EU standard and its conditions<br>2. served on service provider<br>3. Service provider responds within deadlines if possible (data available, no conflicting obligations)<br>4. Produced data introduced as evidence in court; admissibility verified<br><u>Advantages:</u><br>• Reduction of administrative burden for cases in which the receiving authority typically has no own interest because there is<br>○ No connection between the location of service provider establishment and the case (e.g. Facebook in US holding data on German citizen suspected in German case)<br>○ No connection between the data storage |
| Typical use case 2: production of subscriber information, using **EIO** | **EIO**:<br>1. National request prepared and judicially approved based on individual national standard and EIO rules | |

| | Today | Under the proposed new initiative |
|---|---|---|
| | 2. Sent directly to relevant judicial authority in relevant country<br>3. Assessed by receiving judicial authority<br>4. served on service provider<br>5. Service provider responds to executing national authority if possible<br>6. Executing judicial authority sends to requesting judicial authority<br>7. Data introduced as evidence in court; admissibility verified | location and the case<br>○ No connection between the location of the user concerned and the establishment of the service provider<br>○ Low impact on fundamental rights<br>• Increased speed which is essential as data swiftly disappears<br>• Legal certainty for authorities and service providers, some of whom already provide information based on 28 different requests and subject to their own individual specifications<br>• Increased transparency on conditions and process<br>• Ideal scenario: central IT system to channel requests<br>○ would facilitate accountability and audits<br>○ would permit reliable authentication<br>○ would reduce burden on smaller providers<br>○ would allow for plug-in of automated national solutions where those are available (e.g. DE, FR) |
| Typical use case 3: production of subscriber information, using **direct voluntary cooperation** | **Voluntary direct cooperation**:<br>1. National request prepared and judicially approved based on individual national standard<br>2. Sent to service provider<br>3. Service provider reviews based on its individual policy<br>4. Service provider takes a voluntary decision to provide information<br>5. Data introduced as evidence in court; admissibility verified | |

## 2. Summary of costs and benefits

The tables below summarise the costs and benefits for the **preferred option**. Given the limitations created by the lack of available data, the tables have been filled to the extent possible:

| *I. Overview of Benefits (total for all provisions) – Preferred Option (EUR million)* | | |
|---|---|---|
| ***Description*** | ***Amount*** | ***Comments*** |
| ***Direct benefits*** | | |
| Reduction of crime | 3,330 | Main beneficiary of reduction of crime is society at large. |
| Savings in administrative costs | 110 | Main beneficiaries are public authorities in Member States and service providers. Savings arise mainly through increased efficiency in the processes related to cross-border access to e-evidence, both on the public authorities and service providers' side. Includes the total savings over a 10 year period. |
| ***Indirect benefits*** | | |
| | | |
| | | |

The table below summarises the **absolute costs** (i.e. without deducting the baseline costs):

| *II. Overview of costs – Preferred option (million EUR)* | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Policy measure** | | Citizens/ Consumers | | Businesses | | Administrations | |
| | | One-off | Recurrent | One-off | Recurrent | One-off | Recurrent |
| **1** | Direct costs | | | 0 | 24.243 | 0.400 | 27.338 |
| | Indirect costs | | | | | | |
| **2** | Direct costs | | | 0.120 | 22.315 | 0.293 | 25.929 |
| | Indirect costs | | | | | | |
| **3** | Direct costs | | | NA | NA | NA | NA |
| | Indirect costs | | | | | | |
| **4** | Direct costs | | | NA | NA | NA | NA |
| | Indirect costs | | | | | | |
| **5** | Direct costs | | | 1.560 | 22.870 | 1.296 | 26.672 |
| | Indirect costs | | | | | | |
| **6** | Direct costs | | | 0 | 21.553 | 0.672 | 22.508 |
| | Indirect costs | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **7** | Direct costs | | | 0 | 23.660 | 0.648 | 27.550 |
| | Indirect costs | | | | | | |
| **Total preferred option** | Direct costs | | | **1.680** | **114.641** | **3.309** | **130.0** |
| | Indirect costs | | | | | | |

The table below summarises the **net costs** (i.e. the absolute costs minus the baseline costs, so a negative sign indicates savings compare to the baseline):

| ***II. Overview of costs – Preferred option (million EUR)*** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Policy measure** | | Citizens/ Consumers | | Businesses | | Administrations | |
| | | One-off | Recurrent | One-off | Recurrent | One-off | Recurrent |
| **1** | Direct costs | | | 0 | 0.448 | 0.400 | -0.099 |
| | Indirect costs | | | | | | |
| **2** | Direct costs | | | 0.120 | -1.479 | 0.293 | -1.507 |
| | Indirect costs | | | | | | |
| **3** | Direct costs | | | NA | NA | NA | NA |
| | Indirect costs | | | | | | |
| **4** | Direct costs | | | NA | NA | NA | NA |
| | Indirect costs | | | | | | |
| **5** | Direct costs | | | 1.560 | -0.924 | 1.296 | -0.764 |
| | Indirect costs | | | | | | |
| **6** | Direct costs | | | 0 | -2.242 | 0.672 | -4.929 |
| | Indirect costs | | | | | | |
| **7** | Direct costs | | | 0 | -0.135 | 0.648 | 0.113 |
| | Indirect costs | | | | | | |
| **Total preferred option** | Direct costs | | | **1.680** | **-4.332** | **3.309** | **-7.185** |
| | Indirect costs | | | | | | |

As discussed in section 6.2 (quantitative assessment), the costs for national administrations (direct) include:

- One-off costs:
  - Cost of transposing EU legislation in Member States.
- Continuous costs:

- Costs of enforcing the new legislation, in particular when it leads to an increase in the attempts to access e-evidence across borders or an increase in the time that it takes to process an attempt.

The costs for service providers include:

- One-off costs:
  - One-off expenses related to compliance with the measures introduced by the preferred option.
- Continuous costs:
  - Costs of complying with the new legislation, in particular when it leads to an increase in the attempts to access e-evidence across borders or an increase in the time that it takes to process an attempt.

No costs were identified for citizens/consumers.

**ANNEX 4: ANALYTICAL METHODS**

## 1. Qualitative assessment of policy measures

### Non-legislative action

Measure 1: practical measures to enhance judicial cooperation

*a) Judicial cooperation with the US (MLA)*

*Social impact*

The practical measures to enhance cooperation between public authorities in the EU and in the US, in particular the training of EU practitioners and the sharing of guidelines and best practices, would to some extent improve the quality of MLA requests submitted by EU authorities and would therefore both accelerate the treatment of these requests and improve their success rate. On the other hand, the MLA process and the requirements of US law would remain unchanged, which limits the possible impact.

*Economic impact*

Compared to the baseline scenario, the practical measures to enhance cooperation between public authorities in the EU and in the US, in particular the training of EU practitioners and the sharing of guidelines and best practices, would to some extent improve the quality of MLA requests submitted by EU authorities and would therefore save resources for EU and US authorities, in particular for Step 3 in the process depicted in Annex 6 ("*The OIA works with the public authorities of country A to revise the request's format and content to meet US standards"*). In addition to efficiency savings, it was assumed that the number of MLA requests from Member States to the US would also slightly increase.

There would be no impact on non-EU countries, apart from the aforementioned improvement to resources of US authorities and a slight increase in the number of requests to the US.

*Fundamental rights impact*

There would be no impact on fundamental rights compared to the baseline scenario. The absence of clear legal framework for direct cooperation, with the resulting sub-optimal protection of fundamental rights of the persons affected, would not be improved.

The problems affecting cross-border access to electronic evidence would only be very partially addressed through these measures, meaning that the situation would also still negatively affect the fundamental rights of persons who are or may become victims of crime (right to security).

*b) Judicial cooperation within the EU (EIO)*

*Social impact*

The establishment of a platform for online exchange of e-evidence between EU judicial authorities and the creation of an electronic form set out in annex A of the EIO Directive is expected to facilitate judicial cooperation and the exchange of information between judicial authorities of Member States participating in the EIO, allowing them to secure and obtain e-evidence more quickly and effectively, whilst fulfilling the necessary security requirements in a user-friendly manner. In other words, it would allow judicial authorities to benefit from the advantages of modern ICT tools. Furthermore, the platform could provide support to practitioners using it, including through automatic translation services and through references to further materials that can help in formulating a request. It would also facilitate identifying and contacting the relevant counterpart in another Member State.

An additional benefit of the platform would be that it would allow the collection of statistics without requiring any efforts from Member States. In the long term, this would provide a better basis for future evaluation of the instrument and for transparency measures, e.g. providing information on volumes of requests between Member States.

However, the EIO still requires a significant investment of resources from the receiving Member State, which may not be appropriate or necessary for all cases, especially when there is no link with the receiving jurisdiction besides the seat of the service provider. In addition, the EIO's scope is limited to the EU and will not cover data held by service providers headquartered in non-EU countries. Ireland, where a number of US service providers store data and have European headquarters, has not opted in. Denmark does not participate in the EIO.

As for the mutual recognition process, besides including its deadlines, would not be fundamentally changed, meaning that the process will remain longer and more resource-intensive when compared to direct cooperation with service providers.

*Economic impact*

The development of the secure online platform will generate costs for the EU budget and for Member States who will have connect to it. Funding is being made available in the form of grants to help Member States bear these costs. Once the platform is up and running, it will reduce costs for public authorities when requesting electronic evidence to another authority in the EU using the EIO, thanks to the benefits brought by ICT tools.

The electronic form is being developed without creating additional costs for Member States. They will incur some limited costs when disseminating it to their judicial authorities, if it is already used before the platform is up and running.

There would be no impact on non-EU countries.

*Fundamental rights impact*

Within this option, a very limited impact on fundamental rights may be expected with respect to cooperation between public authorities, if at all. The establishment of a secure online platform for authorities to exchange EIO/ MLA requests which ensures confidentiality of all data sets may have a positive effect on the protection of personal data. Otherwise, there would not be any impact compared to the baseline scenario, meaning the situation would not be improved.

Measure 2: practical measures to enhance direct cooperation

*Social impact*

Reasonable improvements in the efficiency of procedures within the existing frameworks can be expected from the practical measures to enhance cooperation between EU law enforcement authorities and service providers. The creation of SPOCs on the public authorities' side will result in more efficient cooperation channels, as can be inferred from the experience of those Member States that have such SPOCs in place. The SPOCs on the law enforcement side provide expertise on the different policies of service providers and can establish relationships with service providers, which for example facilitates the authentication of requests. The centralisation of expertise also improves the quality of outgoing requests. In many cases, these SPOCs also act as a safeguard against futile requests, checking drafts against the various providers' different policies to determine whether or not they are likely to be answered.

Creation of a single point of entry on the service provider's side could also improve direct cooperation with public authorities, both in terms of reliability and efficiency. This has been demonstrated in several successful cases.

Standardisation and reduction of forms on public authorities' side will make it easier for law enforcement to fill them in, and for service providers to authenticate and deal with the request.

Regarding the streamlining of procedures, standards and conditions on the service providers' side would mainly benefit public authorities, who would be faced with less, more consistent requests and policies, and would not have to adapt to a variety of individual service providers' policies, reducing the risk of errors.

Training activities could provide for a better understanding of different policies and procedures used by service providers, and is even more important where streamlining is not achieved. It can help improve the quality of requests and thus reduce the amount of back-and-forth between the different entities involved, which in turn could reduce the average time it takes to receive a response.

Finally, the establishment of an online information and support portal at EU level to provide support to online investigations, including information on applicable rules and procedures, would also avoid that each authority invests in creating a repository of available information. The better public authorities are informed, the higher the quality of

their requests, which would also benefit service providers. An electronic portal could also create more transparency, for example about the volumes of requests, supplementing transparency reports by the major service providers.

All these practical measures would to some extent improve the efficiency of the process and thereby improve access to electronic evidence. This could in turn result in more effective investigations and prosecutions and contribute to improved deterrence for criminals, better protection of victims and improved security for EU citizens.

On the other hand, the room for improvement is limited by the shortcomings of the existing framework, or the absence of a framework. Furthermore, the extent to which these benefits can be achieved largely depends on the willingness of both public authorities and service providers to implement the measures. It cannot be expected that all of them will implement every single measure, and in particular with regard to the streamlining of procedures, it is debatable whether service providers would be willing to go very far.

Moreover, the practical measures can only partly address the identified problems, as they cannot provide solutions to fragmented legal frameworks among Member States. This fragmentation has been identified as a major challenge by service providers seeking to comply with requests based on different national laws. The practical solutions would also not address the need for increased legal certainty, transparency and accountability in direct cross-border cooperation between authorities and service providers, which was highlighted as a key issue by all stakeholders in the expert process. Finally, the proposed measures on cooperation with service providers would only cover providers under US jurisdiction and be limited to non-content data. Therefore, while the overall impact on the effectiveness of criminal investigations should be positive, this measure by itself would not fully address the problem.

*Economic impact*

Regarding the practical measures to improve cooperation between public authorities in the EU and service providers, those that are addressed to public authorities (SPOC, training, standardised forms, online portal) would generate some moderate costs for public authorities,[181] but also improve the quality of requests and would therefore lead to a reduction of resources and costs for service providers and public authorities. Those practical measures addressed to service providers (single points of entry, streamlining of policies) would generate some moderate costs for service providers, in particular if changes to procedures and standard terms of contracts have to be implemented, but public authorities would be faced with less, more consistent requests and policies, and would not have to adapt to a variety of individual service providers' policies, leading to

[181] The costs would depend on how Member States would implement this measure.

cost reductions for them. The improvements are expected to have a slightly bigger impact than the practical measures for judicial cooperation, as they will modify the process. In addition, these practical measures may also lead to a slight shift from judicial cooperation channels to direct cooperation channels based on a better understanding by practitioners of this later channel, generating further savings, and to an increase of the total number of requests made via direct cooperation because requests that were not done previously because of the complexity of the process or a lack of knowledge about the procedure of a particular service provider would now be done.

Given that the practical measures are largely voluntary in nature and do not require participation by all service providers, the economic impact of the practical options should not disfavour SMEs.

*Fundamental rights impact*

There would be no impact on fundamental rights compared to the baseline scenario. There would be no change with regard to legal certainty and individuals' rights in the framework of voluntary cooperation with service providers.

The problems affecting cross-border access to electronic evidence would only be partially addressed through these measures, meaning that the situation would still negatively affect the fundamental rights of persons who are or may become victims of crime (right to liberty and security).

**Legislative action: international agreements**

Measure 3: multilateral international agreements

*Social impact*

A multilateral solution in the framework of the Budapest Convention would have a broad geographical scope going beyond the EU and could possibly also include the U.S, which is currently the main addressee of requests. A broadly applicable international regime would be easier to implement for national authorities and service providers than many divergent regimes. Both judicial cooperation and direct cooperation could be improved by an additional protocol. It would also reflect more faithfully the international dimension of the Internet, even if it would still not cover all states.

As for the impact on the ability of public authorities to investigate and prosecute crime, it will depend on the concrete provisions negotiated and on the participating countries. Once the international agreement would be open for accession, the decision to sign and ratify it would be in the hands of Member States, and they would not be bound by a certain deadline, as would be the case with an EU legislative instrument. For example, the Budapest Convention has been open for ratification since 2001, has been supported by the EU and has acquired recognition as the main international instrument in the field

of cybercrime, yet still two Member States have not ratified it. Furthermore, the mechanisms for ensuring the compliance by Member States with their obligations under an international agreement are arguably less strong than those provided by EU law, notably the scrutiny of the Commission as guardian of the Treaties and the jurisdiction of the ECHR.

*Economic impact*

International solutions that would allow direct cooperation with service providers would lead to a shift from judicial cooperation procedures to direct cooperation with service providers. Similar considerations regarding the economic impact on businesses and on public authorities would apply as for a measure on direct cooperation with service providers.

Regarding the impact on non-EU countries, international solutions are certainly the most favourable options, as they allow agreement to be reached among states on a common approach.

*Fundamental rights impact*

International agreements may be advantageous, as they might allow ensuring an adequate level of protection of fundamental rights, including data protection. They could allow for a joint definition of mutually acceptable conditions, thus reducing conflicts of law, and an appropriate level of fundamental rights protection. Given their wider geographical coverage, they would add value compared to other options.

The (draft) Terms of Reference for the Preparation of a the Additional Protocol to the Budapest Convention on Cybercrime contain a mandate to prepare text on safeguards (including data protection requirements) for cross-border access to information. It is, however, too early to assess the level of fundamental rights protection that would be achieved by the Additional Protocol.

Measure 4: bilateral international agreements

*Social impact*

Bilateral agreements would have the advantage of creating more legal certainty on the basis and process for direct cooperation with private parties in non-EU countries, especially if they follow parallel choices made within the EU. If one looks at the example of the draft US-UK agreement, its major benefit would be to allow service providers under US jurisdiction to provide content data to EU public authorities, which is currently not possible. This in particular could not be achieved by EU legislation alone, as it would create a conflict of law with US law. Another advantage would be that the provisions of the EU-US Umbrella Agreement would be applicable to such an agreement.

But both bilateral and multilateral agreements are uncertain; it could take years, if at all, to reach an agreement, and it would depend on the non-EU countries involved.

*Economic impact*

International solutions that would allow direct cooperation with service providers would lead to a shift from judicial cooperation procedures to direct cooperation with service providers. For an EU-US agreement, this would mean content data could also be obtained via direct cooperation. Similar considerations regarding the economic impact on businesses and on public authorities would apply as for a measure on direct cooperation with service providers.

Regarding the impact on non-EU countries, international solutions are certainly the most favourable options, as they allow agreement to be reached among states on a common approach.

*Fundamental rights impact*

Like multilateral agreements, bilateral international agreements may be advantageous, as they might allow ensuring an adequate level of protection of fundamental rights, including data protection. They could allow for a joint definition of mutually acceptable conditions, thus reducing conflicts of law, and an appropriate level of fundamental rights protection.

In the framework of bilateral agreements such as with the US, it would most likely be easier to negotiate an adequate level of fundamental rights protection. Regarding data protection, the Umbrella Agreement would apply to an EU-US agreement, ensuring an equivalent level of protection as in the EU of the right to data protection and privacy.

**Legislative action: direct cooperation**

Measure 5: European Production Order

*Social impact*

This measure would create a mechanism to allow judicial authorities to compel certain foreign service providers to provide information, in a similar way to that of domestic providers, subject to specific conditions. It would bring significant benefits in terms of efficiencies both compared to judicial cooperation channels and to voluntary cooperation that exists with US providers on non-content data.

While the EIO Directive is expected to improve cooperation among Member States compared to the instruments replaced by it, notably the 2000 MLA Convention, it is certainly a less efficient channel to obtain electronic evidence than direct cooperation with service providers, since the EIO was not specifically made for the purpose of improving cross-border access to e-evidence. Direct cooperation with service providers is more comparable to domestic production orders: it involves fewer actors (no executing authority) and is limited to a specific type of evidence, which means that e.g. the form that would be used in the European Production Order could be designed for the specific

needs of electronic evidence and would be much shorter than the one to be used for an EIO. Deadlines for the execution of European Production Orders would be significantly shorter than the ones for the EIO: they only need to give service providers sufficient time to obtain the evidence, while the deadlines in the EIO include the time needed for many more steps (the executing authority needs to check the EIO and the grounds for refusal, and then it issues a domestic production order to the service provider according to their own provisions; the service provider needs to obtain the evidence and send it to the executing authority; and the executing authority sends it to the issuing authority, possibly after having re-checked the grounds for refusal on the basis of the evidence obtained).

As described in the report, there is a strong demand from Member States for an EU instrument in this area, which reinforces the above arguments that the EIO cannot fully address the challenges of cross-border access to e-evidence, one of which is the need to access e-evidence across borders faster. Only the creation of a new instrument for e-evidence would be able to achieve these benefits by fundamentally departing from the traditional mutual recognition procedure on which the EIO is based, which involves an issuing authority and an executing authority in the Member State in which the investigative measure is to be carried out. Because the direct cooperation is inspired by the existing voluntary cooperation with US service providers, which has de facto become the main channel to obtain electronic evidence nowadays, the creation of an additional instrument would not bring more complexity to the current situation, but, on the contrary, provide for a clear legal framework for the direct cooperation channel. Furthermore, the new instrument would be **complementary** to the EIO. There may be situations, e.g. when several investigative measures need to be carried out in the executing Member State, where the EIO may be the preferred choice for public authorities.

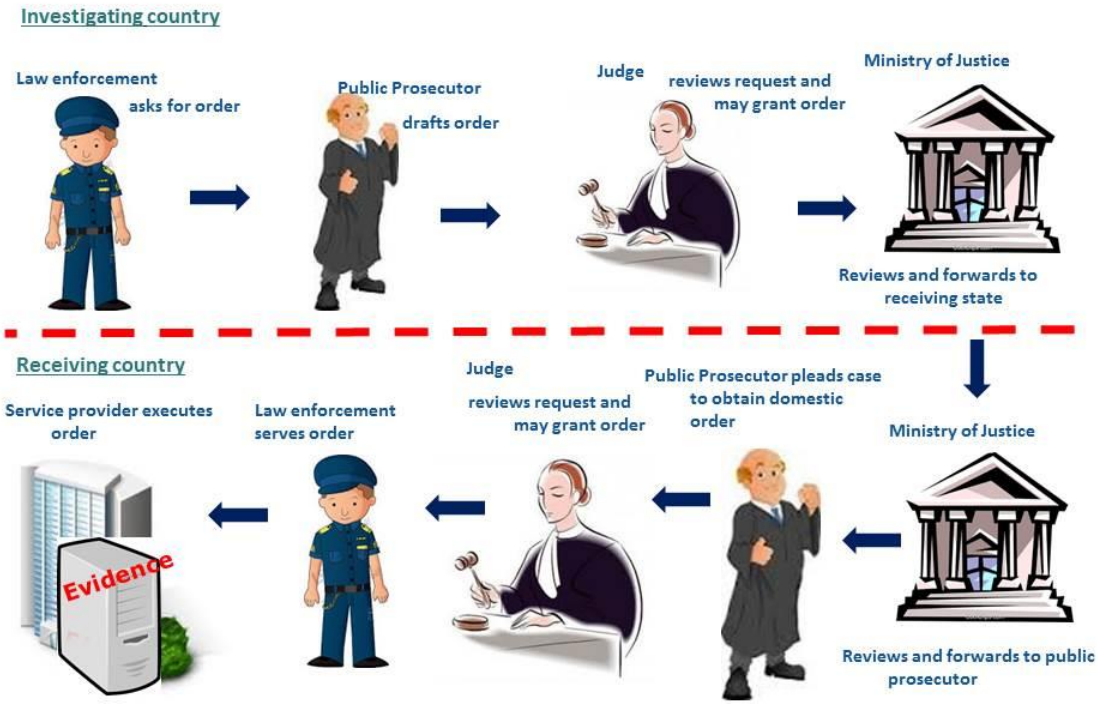
The major benefits of such a mechanism would be to provide a direct channel for the large majority of cases where the interest of the receiving country in the investigation is small to non-existent, to accelerate the process compared to formal judicial cooperation tools, and to create a mandatory framework compared to the voluntary cooperation with US providers. The Production Order would be enforceable vis-à-vis service providers, meaning that the success rate would be significantly higher than under the current voluntary framework (where it is currently estimated to be below 50%). Because of the conflict with US law, it would not allow EU judicial authorities to obtain content data. This measure would take some pressure off the MLA channel, by establishing a separate formal route for requests relating to non-content data. It is therefore expected that it would also have a positive effect on the quality of requests and the response time for MLA requests.

With regard to EU providers, it would introduce a new mechanism that does not currently exist in most Member States, leading to a significant shift from judicial cooperation channels to more efficient direct cooperation channels. Creating such an EU framework would provide greater legal certainty for all stakeholders and reduce the level of

complexity and fragmentation for US service providers. Service providers would have legal certainty as to their duties, and their users would have clarity as to the service providers' obligations.

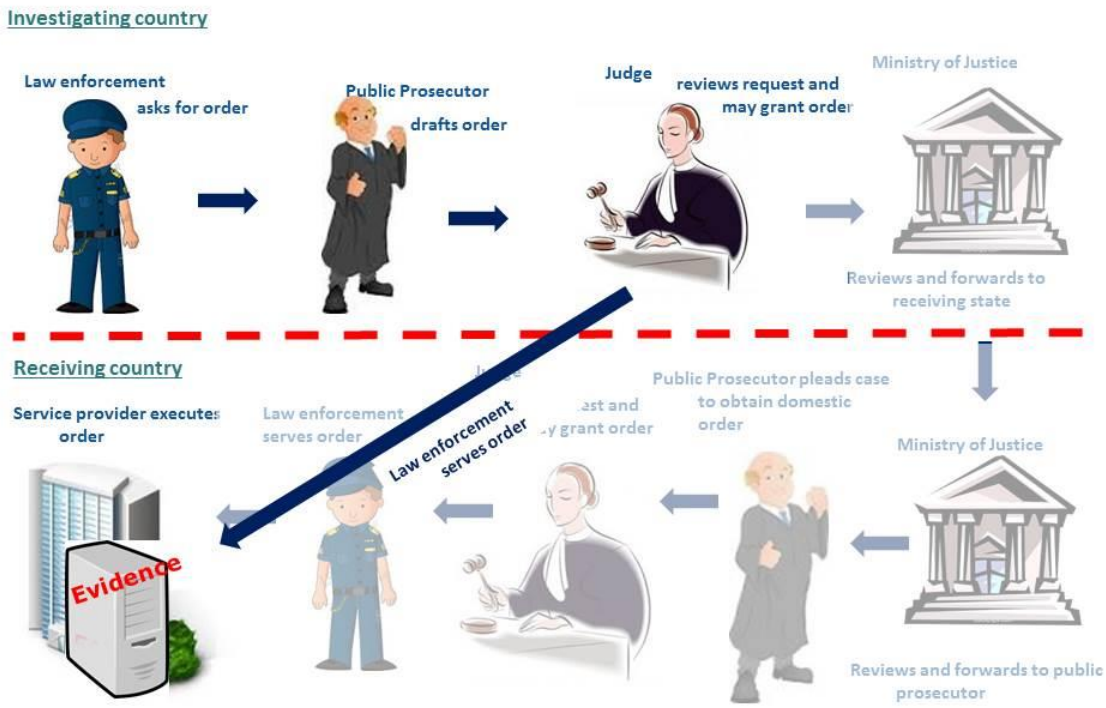
The change in procedure as compared to MLA is illustrated below:

Diagram 1: MLA




As evident from the diagram, the law enforcement request cycles through a number of actors and the evidence (if any) follows the same process in reverse order (not shown here).

Diagram 2: European Production Order




Measure 5 would provide for a direct service of the order on a service provider and direct response with the evidence (if any). Overall, this may result in evidence being obtained more swiftly and also in cases in which public authorities would not even have tried to obtain it currently because of the cumbersomeness and duration of formal judicial cooperation procedures. It would also be based on agreed connecting factors (being established in the EU or offering services in the EU). If the new instrument provides for an effective way to obtain e-evidence in cross-border situations, this would also reduce Member States' incentives to use diverging connecting factors, to the benefit of both other States and of service providers.

The framework could also reduce issues experienced by authorities in some Member States with the admissibility in court proceedings of electronic evidence obtained through direct cooperation with service providers.

*Economic impact*

- General economic impact of legislation on direct cooperation (EPO, EPR, EPRO)

If an efficient procedure is implemented to obtain cross-border access to electronic evidence, a significant proportion of judicial cooperation requests would shift to direct

cooperation as the more efficient instrument. This concerns predominantly intra-EU requests, as direct cooperation was previously not possible here, whereas a change in numbers regarding direct cooperation with US providers is not expected. In addition, public authorities will attempt to obtain such data also in cases where today they may have been discouraged even to try due to the cumbersome procedure required. As a result, an increase in the total number of direct cooperation requests being issued by public authorities could therefore be expected from a measure on direct cooperation with service providers.

In addition to this increased number of requests for data for the purpose of criminal investigations or procedures, European service providers would also receive such requests directly from public authorities from other Member States, instead of from their own public authorities. They would be subject to two sets of requests, domestic ones and European ones. This could possibly create some distrust on their side, and uncertainty as to the applicable legal framework. To mitigate such risks, the proposal would introduce a unique form used by all public authorities throughout the Union for cross-border cases, putting an obligation on issuing authorities to translate requests into the local language of the service provider (which should be facilitated by the form), helping to ensure authenticity of requests and providing clarity as to the applicable conditions for issuing, safeguards and legal remedies. US service providers, which are currently already replying to direct requests from Member States' authorities, and other non-EU service providers would benefit from a more harmonised legal framework for cross-border requests, instead of 28 different ones.

SMEs would be be faced with a relatively higher administrative burden when faced with production orders from other Member States (see Annex 13). On the other hand, they would benefit more from a clear legal framework in the EU and a unique procedure and form applied by all Member States.

For both the public and the private sector, administrative and compliance costs arise from implementing new legislation. Service providers would also have to adapt their standard terms and conditions to the new legal framework.

For public authorities, a legal framework for direct cooperation with service providers would introduce many efficiencies compared to judicial cooperation channels. When acting as issuing authority, they would apply the same procedure, whether the service provider is established inside or outside of the Union. But the direct cooperation would also limit the role of the executing authority to situations of sanctioning in cases of non-compliance with a Production Order; for the request for data, there would only be one public authority involved in the issuing State, instead of two, as for judicial cooperation channels. This will reduce the costs for those authorities that would otherwise have been asked to recognise and execute judicial cooperation requests. Compared to the current direct cooperation, the additional safeguards such as judicial authorisation will slightly

increase the costs to issue one request compared to the current practice with US providers.

Both the public and the private sector would benefit from a common framework creating more legal certainty and mutual trust between the public and the private sector, and reducing the number of applicable laws. Harmonised definitions of types of electronic evidence would provide for a common understanding and legal certainty for all stakeholders concerned by the instrument.

- Economic impact specific to European Production Orders (sub-options EPO and EPRO)

A major difference for US providers compared to the current situation would be the mandatory nature of production orders. It would no longer be up to them to decide whether or not to provide the requested data. Arguably, this should reduce the costs they currently incur in checking the legality of requests obtained from foreign public authorities, but the number of requests they would reply to would increase. As the measure would also include deadlines for service providers to respond, this may require service providers to allocate additional resources to the task. The costs and administrative burden for the public sector relating to requests to service providers that are not replied to or replied with a notable delay will be significantly diminished.

An inherent risk of introducing a mandatory framework with a large scope would be the creation of conflicts of laws for non-EU service providers: between the obligation to comply with the production order, and the obligation to comply with domestic law provisions prohibiting the disclosure of data to foreign public authorities outside of an MLA procedure. This can result from the law of a non-EU country applicable to the data and/or the service provider, which may prohibit or restrict/condition such disclosure of data to foreign law enforcement. For example, the US Electronic Communication and Privacy Act prevents US companies from sharing content data directly with foreign law enforcement. The need to avoid creating new conflicts of laws was raised repeatedly by service providers, civil society and some Member States during the consultation phase of this initiative. This issue could be addressed by means of a dedicated procedure for reviewing such conflicting obligations in the issuing Member State. In case of a conflict situation with the laws of a non-EU country the service provider could invoke that conflict on the basis of a reasoned refusal to comply. In case of disagreement, a court could be asked to review the case. This could also trigger a procedure involving consultation with the non-EU country's authorities. In the context of such a procedure, the judge could uphold the order or order preservation of the data while awaiting mutual legal assistance from the authorities of the non-EU country.

A one-off cost would be generated by the obligation to designate a legal representative in the Union. For service providers already established in the Union, this would amount to little more than to designate a single point of entry. Service providers not established in

the Union would have to mandate somebody in the Union to carry out this task. In particular for SMEs, there is a fear that this could represent an important burden. On the other hand, this legal representative could be shared between service providers, and the legal representative may accumulate different functions (e.g. GDPR or ePrivacy representatives in addition to the production order legal representative).

Improved access by EU authorities to e-evidence could affect business models chosen by service providers, in particular where data location and access to this data is an important factor for customers. Differentiation can be made between B2B customer business models (e.g. Microsoft's corporate services) and B2C models (Google and Facebook's provision of individual accounts), the latter's customers would have less at stake with regard to data localisation issues. To mitigate this risk, the principle of "controller first" could be introduced in the instrument, which means that the business customers would be asked first to provide the data.

*Fundamental rights impact*

- General fundamental rights impact of legislation on direct cooperation (EPO, EPR, EPRO)

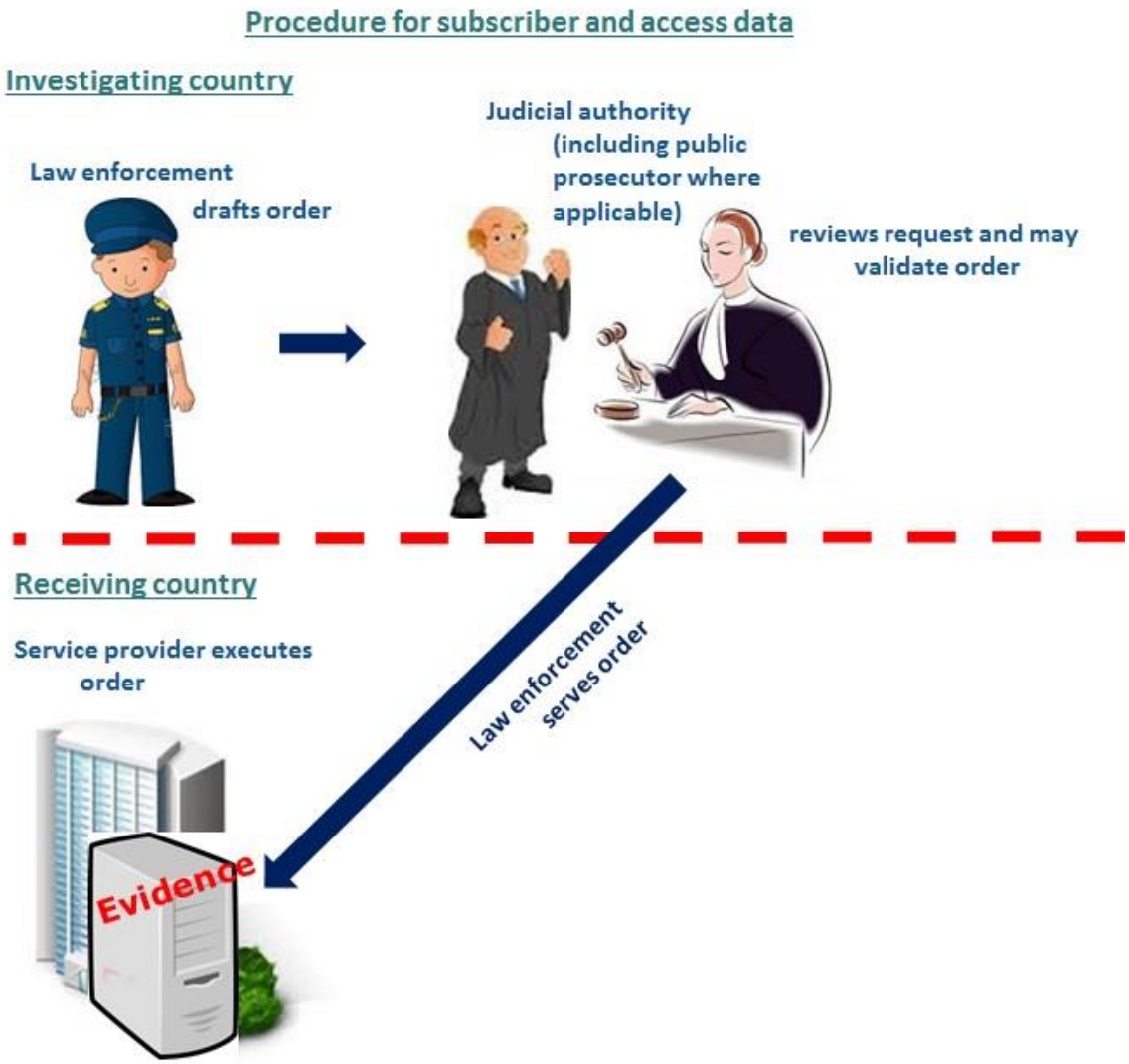
Measures to facilitate direct cooperation of public authorities with service providers may have a considerable impact on fundamental rights, as it would allow public authorities to access data that is not publicly available and that is, in most cases, personal data. However, it has to be noted that, contrary to data retention frameworks, access to data for the initiative at hand should always take place in the framework of a concrete criminal investigation or concrete criminal proceedings, which is a very different starting point in terms of the fundamental rights impact.

As regards the protection of the rights of the person whose data is sought, the protection of fundamental rights would be ensured primarily by the procedure in the issuing Member State, which is subject to national law and to applicable EU law (notably the acquis on the rights of accused and suspected persons, in particular Directive 2012/13/EU on the right to information in criminal proceedings).

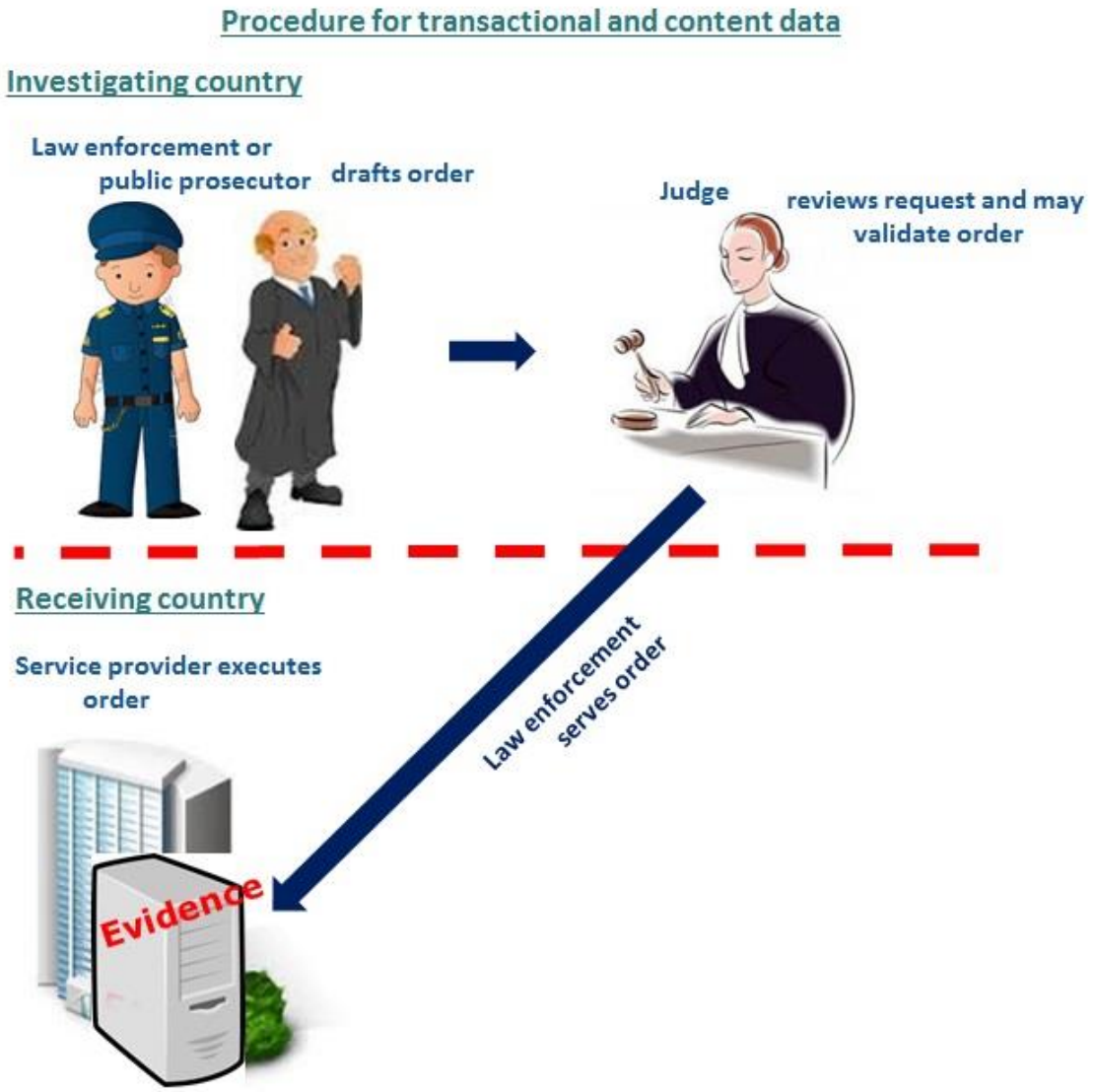
To ensure the protection of the rights of the persons affected, the European Production Request and the European Production Order would include additional safeguards mentioned in section 5. The intervention of a judicial authority when the request or order is issued will ensure that the legality of the measure has been checked and that the order does not infringe on fundamental rights. As the measure would not include any limitation to serious forms of crime, the issuing judicial authority should be required to ensure in the individual case that the European Production Order is necessary and proportionate, including in view of the gravity of the offence under investigation. This will prevent that a European Production Order is issued in a situation where it would be disproportionate in view of the lack of seriousness of the offence, but avoiding at the same time that the instrument could not be used at all for certain types of crimes which may become

important for other reasons in specific cases, e.g. because affecting a high number of victims. Depending on the data category, the definition of "judicial authority" could be further restricted, as illustrated below:

Illustration 1: For subscriber and access data, an order could be validated also by a prosecutor:



For meta and content data, prosecutors would not be able to validate orders, as shown in Illustration 2:




The possibilities of an effective remedy for persons whose data is being requested would also have to be addressed. Some provisions of the receiving State, e.g. on immunities and privileges of certain professions such as lawyers and the principle of double criminality would also have to be taken into account during trial in the issuing State.

Of particular importance, given the type of measure, is the need to guarantee the fundamental rights to data protection and privacy. Subscriber information, metadata and content data are, at least in the majority of cases, personal data, and are thus covered by the safeguards under the EU data protection acquis. In the context of the possible measures, the type of data – as well as other factors such as for instance the volume of data to be accessed or the type of investigative measure – may be relevant for assessing the intensity of the interference with the fundamental right to data protection, and

therefore for determining whether such interference respects the principle of proportionality. The judicial authority would be required to check that the data sought is necessary for and is limited to what is necessary and proportionate to the purpose of the proceedings, also in view of the nature and gravity of the offence under investigation (petty crime versus more serious offences) and in view of the data category. Additionally, as for the right of the data subject to be personally informed about the measure, any restriction of such right would have to take into account the requirements of Article 13 of the Police Directive.

- Fundamental rights impact specific to European Production Orders (sub-options EPO and EPRO)

Because the production order would be a mandatory measure, and it would also encompass the obligation to designate a legal representative, the measure could also affect the rights of service providers, in particular the right to freedom to conduct a business. The fact that third parties such as service providers, who hold evidence that may be relevant for a criminal investigation, have to cooperate with public authorities is widely recognised. To protect them from requests that are erroneous, the proposal could include a right for the service provider to raise certain types of errors, e.g. if the order has not been issued by a judicial authority. The obligation to nominate a legal representative mainly affects service providers which offer their services in Europe, but have no physical presence here. For service providers established in the EU, this obligation would not have any far-reaching impact, as it would at most oblige them to reorganise their internal business processes to have all requests transit through the legal representative. The legal representative already exists in other instruments, e.g. the GDPR and the ePrivacy proposal, and is necessary to allow for the instrument to work with regard to foreign service providers not established in the EU.

Because a measure on production orders would significantly improve cross-border access to electronic evidence, it would also improve the rights of persons who are or may become victims of crime.

One of the risks of a mandatory approach would be that it could inspire non-EU countries which do not have fundamental rights safeguards in place that can be considered comparable to ours, including in the field of data protection, to introduce a reciprocal obligation for EU service providers active on their territory. The potential consequences of such measures is that it could undermine the high level of protection ensured by the EU acquis for data subject to it, by making this data potentially available to such non-EU countries. Providers would find themselves in a conflict of obligations between the data protection prohibition to share the data and a possible production order issued by the authorities of the non-EU country. This could be mitigated first by providing for a high level of fundamental rights protection in the instrument (leading by example), and second by complementing the requirement of production orders with an international framework

to channel similar requests from non-EU countries, through the Additional Protocol to the Budapest Convention under negotiation, and ensuring that the necessary safeguards are put in place in that process. However, the outcome of the negotiations are not yet clear. Another, more controllable solution would be to provide for a conflicts of law clause that would give a role to the law of the non-EU country. If that were to be put in place reciprocally as well, it would allow providers to raise conflicting obligations as a possible obstacle to compliance. This clause would also be a means to achieve international comity (see Box 4). Because the conflicting laws of non-EU countries would be taken into account, the Union and Member States could claim that these countries should do the same when requesting electronic evidence from an EU service provider, e.g. when there is a conflict with the EU data protection regime. This would mitigate the risk that our data protection acquis is undermined by non-EU countries.

Measure 5*: European Production Request

*Social impact*

A measure on Production Requests would increase legal certainty for requests on non-content data addressed to service providers in the US, compared to existing voluntary cooperation channels. For content data, as long as the US law does not permit direct cooperation, the production request would not change the current situation. For other situations, the production request would clarify that this form of cooperation is possible and turn it into a legitimate tool, creating legal certainty and expanding swift access. Notably for EU providers, the measure would allow them voluntarily to provide non-content and content data to law enforcement authorities from other Member States upon request, thereby creating a new, faster channel to access data.

The competence for service providers to reply to requests would also provide for improved conditions for cross-border cooperation with service providers to obtain electronic evidence within the EU.

However, the measure would still depend on the willingness and commitment of service providers to cooperate, as production requests are a voluntary mechanism. Extrapolating from the current success rate for voluntary cooperation of the large service providers, it would at maximum allow getting the data in about 50% of cases: the service providers which already provide access that is voluntary from the perspective of US law do so on the basis of a very large market share in Europe and many requests, allowing for economies of scale and at the same time creating a larger motivation for compliance with EU Member States' law enforcement. The same cannot be said for smaller, EU-based providers who would be faced with difficult choices about how to position themselves and about investment if presented with a voluntary instrument.

The lack of enforceability would require further action through traditional channels if service providers did not cooperate with a request. Creating a legal basis for a

competence to initiate production requests and to allow service providers to respond to requests alone is thus not likely to fully address all identified problems and objectives.

*Economic impact*

See the analysis above on the general economic impact of legislation on direct cooperation.

*Fundamental rights impact*

See the analysis above on the general impact on fundamental rights of legislation on direct cooperation. In addition, because there would be no obligation on service providers to comply with a EPR or to nominate a legal representative, they would not be affected in their right to conduct a business.

The above analysis suggests that, if applied with proportionality and complemented with the proposed safeguards, all sub-options of the measure in this policy option are compatible with fundamental rights requirements.

Discarding of measure 5*:

Compared to the European Production Order, this measure is less effective, in particular because of the lack of a possibility to execute it. At the same time, it does not bring additional benefits compared to the European Production Order. This measure is therefore discarded. This is also in line with the preference expressed by Member States' experts for a mandatory measure.

Measure 5**: European Production Request and Order

*Social impact*

A combination of Production Orders for non-content data and Production Requests for content data would combine the benefits and limits of the EPO and the EPR. It is a less efficient option compared to the EPO, but a more efficient solution compared to EPR.

*Economic impact*

See the analysis above on the general economic impact of legislation on direct cooperation and the specific aspects to European Production Orders.

*Fundamental rights impact*

See the analysis above on the general impact on fundamental rights of legislation on direct cooperation and the specific aspects to European Production Orders.

Discarding of measure 5***:

Even if this measure is more efficient than the European Production Request, it is still less effective than the European Production Order, while not bringing additional benefits.

**This measure is therefore discarded**. This is also in line with the preference expressed by Member States' experts for a mandatory measure.

Measure 6: access to data without individualised review (WHOIS)

*Social impact*

For WHOIS data that service providers make available specifically for access by authorities through a system of databases without individual review by the service provider, legislation on direct cooperation could provide for a legal basis to perform searches in the system. Such a legislative basis would enable authorities to continue to access the system in the same manner even when it is password-protected and no longer publicly available. Providing a new legal basis for the changed circumstances would preserve an essential tool in online investigations and would prevent a significant decrease in effectiveness of investigations in view of the high frequency of these look-ups.

*Economic impact*

If a legal basis and framework is provided for access to the WHOIS, authorities might be able to maintain the level of access they benefit from today, generating no new costs for the authorities aside from the cost of implementing new legislation. Similarly, such a legal basis would be cost-neutral for the provider side. This measure would also prevent an avalanche of orders to service providers to produce the data, which might otherwise generate significant costs for both sides due to the resulting increase in volume of total requests.

*Fundamental rights impact*

The impact on fundamental rights of the legal base for access to the WHOIS would be small. Creating such a legal base would also indirectly allow the system to move to a tiered-access model as it could still ensure the vital public policy interests at stake. This in turn would have a positive effect on individuals' fundamental right to privacy, as their personal data is no longer publicly available.

**Legislative action: direct access**

Measure 7: legislation on harmonised safeguards for direct access

*Social impact*

The option to legislate on direct access, including a set of conditions and safeguards, as described above, could improve the capacity of public authorities to investigate and prosecute crimes according to the following considerations:

Enabling Member States to put in place a legal base for direct access with a harmonised system of conditions and safeguards would provide a basis for those Member States who have chosen to enable direct access to adapt them – where necessary – to be mutually

acceptable among Member States. It would furthermore provide for clarity on the conditions and safeguards that apply regardless of EU Member State.

It would also contribute to avoiding tensions and increasing mutual trust among Member States and therefore improve judicial cooperation in general.

Those Member States where such direct access to data is currently not possible when the location of the data is not known[182] would be free to introduce national measures to regulate direct access to data. A slight increase in the number of direct access attempts could therefore be expected. This could improve the effectiveness of investigations, as alternative judicial cooperation channels are only possible if the location of the data or of the service provider is known, and would not in all cases allow receipt of the data because of longer procedures.

The conditions and safeguards would furthermore help provide legal clarity to those Member States where the legal situation is unclear or subject to divergent interpretation.

Implementing conditions and safeguards in the context of already existing national solutions might lead to additional time for public authorities to ensure compliance. This could have an adverse effect on the effectiveness of investigations. However, based on the expert input received during the consultation process, any decrease in effectiveness was regarded as being outweighed by the harmonised framework for conditions and safeguards that would ensure the mutual acceptance of Member States.

Some non-EU countries may however object to foreign law enforcement accessing data that later can be identified as having been stored in their territory at the time of copying.

*Economic impact*

A legislative measure on direct access will not impose any new obligations or administrative burdens on service providers, as they are not involved during direct access.

For public authorities, administrative and compliance costs arise from implementing new legislation. Alternative judicial cooperation channels are only possible if the location of the data or of the service provider is known. However, because of the specific conditions for these kinds of measures, it is not expected that the cases will be numerous. Therefore the impact should be moderate.

This measure should not have any cost effect on non-EU countries.

*Fundamental rights impact*

This option would allow public authorities to access data that is not publicly available and that is, in most cases, personal data. However, the intrusiveness is already inherent to

[182] According to replies received to a questionnaire in summer 2016, this concerns 8 Member States.

the national investigative measure, such as the search and seizure measure. The EU legislation would allow public authorities to also access data stored remotely if it is not clear whether it is stored on their territory, where this is not yet provided for in national law, i.e. it would widen the scope of the measure to data to which they may not necessarily have had access until now. But whether the data is stored on a device or remotely in the cloud, on the territory of the investigating Member State or in a non-EU country, should not be a relevant factor regarding the fundamental rights protection of the data subject (which should be adequate), nor regarding the sensitivity of access by public authorities.

The protection of fundamental rights of the person whose data is sought is ensured by the procedure in the issuing Member State, which is subject to national law and to applicable EU law (including the acquis on the rights of accused and suspected persons, in particular Directive 2012/13/EU on the right to information in criminal proceedings). As the measure would preserve the competence basis for any such measure in national law, all safeguards and conditions set out by the respective national law would be preserved by this instrument (including thresholds, privileges etc.).

The measure would include additional conditions and safeguards mentioned in section 5 to ensure that the use of this measure remains exceptional, such as the requirement that the data sought is necessary for the investigation and the measure is limited to what is necessary and proportionate to the purpose of the proceedings, also in view of the nature and gravity of the offence under investigation.

Where direct access takes place without the knowledge of the user concerned, user notification needs to be ensured when not already provided for by the national investigative measure and national legislation implementing the Data Protection Directive.

The above analysis suggests that, if applied with proportionality and complemented with minimum conditions and safeguards, the measure in this policy option is compatible with fundamental rights requirements.

It should be noted that this approach could also inspire non-EU countries to introduce a similar possibility for their law enforcement authorities. This may lead to fundamental rights issues resulting from non-EU country access to personal data of EU citizens without ensuring due process and legal safeguards comparable to EU standards. Contrary to the EPO, it is not possible to address this issue with a provision like the conflicts of law clause.

At the same time, a number of non-EU countries would not need to rely on EU legislation, as they may have already put in place other approaches to ensure access to data, such as data localisation obligations or a more expansive set of investigative measures, including possibilities for investigators to directly access data, going further than what is proposed here. In that light, creating a framework for access to electronic

evidence that builds on the robust protections already provided for under EU law and including specific safeguards could also set a positive example.

Measure 7*: Recommendation on cross-border online searches

*Social impact*

Providing conditions and safeguards for direct access, as described above, could provide a basis for those Member States who have chosen to enable direct access to do so in a manner that is mutually acceptable among Member States.

It could also contribute to avoiding tensions and increasing mutual trust among Member States and therefore improve judicial cooperation in general.

Those Member States where such direct access to data is currently not possible when the location of the data is not known[183] would be free to introduce national measures to regulate direct access to data and could take into account the recommended conditions and safeguards in doing so. The conditions and safeguards could furthermore provide support to those Member States where the legal situation is unclear or subject to divergent interpretation.

However, these positive impacts would only apply to the extent to which Member States choose to implement the recommendation. Any positive impact would be limited if only a small number of Member States follow the recommendation as they would not be able to rely on a common framework applying to all Member States that make use of direct access. These same considerations also apply when it comes to increasing mutual trust, as a recommendation might not be successful in addressing disparities between Member States. It might indeed contribute to further fragmentation if implemented only partially or in a disparate or inconsistent manner.

*Economic impact*

A recommendation will not impose any new obligations or administrative burdens on service providers or authorities.

For Member States choosing to implement (parts of) the recommendation, administrative and compliance costs arise from implementing new legislation or adapting existing legislation, in line with the recommendation.

This measure should not have any effect on non-EU countries.

*Fundamental rights impact*

This measure would not introduce any new legal basis for direct access but rather provide a non-binding list of conditions and safeguards mentioned in section 5 to ensure that the

[183] According to replies received to a questionnaire in summer 2016, this concerns 8 Member States.

use of direct access remains exceptional, such as the requirement that the data sought is necessary for the investigation and the measure is limited to what is necessary and proportionate to the purpose of the proceedings, also in view of the nature and gravity of the offence under investigation.

Where direct access takes place without the knowledge of the user concerned (remote access), the recommendation would furthermore suggest that user notification needs to be ensured when not already provided for by the national investigative measure.

Such conditions and safeguards could have a positive impact on the fundamental rights impacted by national measures allowing for direct access. However, given the non-binding nature, the impact of the measure would largely depend on Member States' willingness to adopt the proposed conditions and safeguards. Its effectiveness in further reducing the fundamental rights impact of any national legal basis for direct access could thus be limited.

Discarding Measure 7*:

Given its nonbinding nature, the effectiveness of this measure would likely be limited. Its main benefit would lie in further increasing fundamental rights protections; however, these possible benefits are outweighed by the lack of legal certainty and the added risk of fragmentation. The measure is therefore discarded.

## 2. Qualitative comparison of policy options

The options are compared below through listing positive (+), negative (-) and 'no-change' (0) impacts compared to the baseline, and in absolute terms, to allow scoring the baseline too. The score system ranges from -3 to +3.

**Option 0: baseline**

| Criteria | Assessment | Score |
|---|---|---|
| **Effectiveness/ social impact** | Law enforcement authorities' capacity to investigate and prosecute crime will not improve, but is rather expected to be reduced due to growth of electronic data and the move away from publicly available data, requiring judicial cooperation procedures where formerly a direct lookup sufficed. Even more time would be spent to access e-evidence across borders, and the number of cases which could not rely on electronic evidence would increase.<br>- Cooperation between public authorities would probably take longer, given the unlikelihood of a growth in resources to deal with the increased number of MLAT/EIO requests.<br>- In the absence of a mandatory legal framework, direct cooperation between service providers and public authorities is likely to suffer under the strain of the | **-3** |

| | | |
|---|---|---|
| | increasing number of requests.<br>- Without a clear EU framework defining jurisdiction in cross-border access to e-evidence, Member States are likely to introduce different practices and legislative instruments at national level which would lead to fragmentation and more conflicts of laws. This would hamper effective cross-border cooperation. | |
| **Efficiency** | Expected increase in number of requests will put increased burden and costs on both public authorities and service providers. | **-1** |
| **Competitiveness** | - Lack of legal certainty imposes burden on companies, in particular SMEs, in which they must discern which law governs in the context of cross-border requests and where they may be liable to their users. | **-1** |
| **Fundamental rights and freedoms** | .++ For judicial cooperation, a double check takes place by issuing authority and executing authority.<br>- Absence of legal framework for direct cooperation with service providers for non-content data may interfere with fundamental rights of the data subject; some service providers check legality of request for data according to law of issuing State.<br>0 In the absence of a mandatory regime, the rights of service providers are not affected.<br>+ Direct access takes place based on national law, high level of protection.<br>- The problems affecting cross-border access to electronic evidence negatively affect the fundamental rights of persons who are or may become victims of crime (right to security). | **0** |
| **Impact on 3rd countries and international relations** | - Increased burden also for non-EU countries'authorities as number of MLA procedures increase.<br>- Increased risk of conflicts of law for service providers due to diverging national solutions.<br>0 No impact on reciprocity. | **-1** |

**Option A: non-legislative action**

| Criteria | Assessment | Score |
|---|---|---|
| **Effectiveness/ social impact** | More effective investigations and prosecutions, savings for both public authorities and service providers.<br>+ Foreseen training and sharing of guidelines and best practices as well as creation of SPOCs or single points of entry should improve the quality and the treatment of requests, to the benefit of both for judicial cooperation channels and for voluntary cooperation.<br>+ Streamlining of procedures and standards could increase effectiveness of voluntary cooperation channels.<br>+ Increase in total number of requests because requests that | **-2** |

| | | |
|---|---|---|
| | were not done previously because of the complexity/ lack of knowledge about the procedure would now be done, i.e. more evidence available for investigations and prosecutions.<br>- Effectiveness of measures will depend on willingness to implement them.<br>But improvements will not affect shortcomings of legal framework.<br>-- None of the proposed practical measures solve the issue of fragmentation linked to the divergent legislation EU Member States: they will not be sufficient: i) to provide to EU citizens/residents the same standard of transparency and rule of law regarding the disclosure of their data, which depend on the conclusion and the content of agreements between their Member State(s) and their provider(s); ii) to reduce the different approaches among private companies offering the same services, as the legal framework and obligations vis-à-vis law enforcement/judicial authorities depend on their nationality (EU or US) and their statute (internet providers or telecom).<br>--The issue of transparency and accountability of service providers and law enforcement in the context of direct requests is not addressed.<br>+ The platform and form to exchange EIO requests will allow public authorities to secure and obtain e-evidence more quickly and effectively, whilst fulfilling the necessary security requirements;<br>+ The platform would enable better collection of statistics, indicators and evaluation of the instrument.<br>- EIO's scope is limited to EU territory, and will not cover service providers headquartered in non-EU countries, nor in Ireland and Denmark.<br>- The mutual recognition process would not be fundamentally changed, meaning that the process will remain longer and more resource-intensive when compared to direct cooperation with service providers.<br>- The issue linked to access to the WHOIS database would not be solved. | |
| **Efficiency** | - Administrative costs would be incurred by public authorities and service providers for implementing practical measures.<br>+ Practical measures may lead to a slight shift from judicial cooperation channels to direct cooperation channels, generating savings<br>+ Carrying out the measures would improve the quality of requests, leading to a reduction in resources for both public and private entities.<br>+ SPOC system and standardised procedures could reduce burden on service providers and public authorities.<br>EIO platform and form: | **-0,5** |

| | | |
|---|---|---|
| | - Initial increase to baseline costs for EU budget and Member States in developing and connecting to the secure online secure platform.<br>++ Once platform is up and running, costs will be reduced compared to the baseline.<br>- Member States public authorities will incur some costs in disseminating the electronic form to their judicial authorities, if it is already used before the platform is up and running. | |
| **Competitiveness** | 0 No impact compared to baseline scenario | **-1** |
| **Fundamental rights and freedoms** | 0 Only limited impact can be expected from platform compared to the baseline, no impact from the other practical measures.<br>(+) Setting up a secure online platform for authorities to exchange EIO/ MLA requests which ensures confidentiality of all data assets may have a positive effect on the protection of personal data. | **0** |
| **Impact on 3rd countries and international relations** | 0 Limited impact compared to baseline scenario<br>(+)Training of EU practitioners in US law requirements will reduce costs also for US authorities involved in MLA procedures | **-0,5** |

**Option B: Option A + international agreements**

| Criteria | Assessment | Score |
|---|---|---|
| **Effectiveness/ social impact** | More effective investigations and prosecutions, savings for both public authorities and service providers.<br>+ Foreseen training and sharing of guidelines and best practices as well as creation of SPOCs or single points of entry should improve the quality and the treatment of requests, to the benefit of both for judicial cooperation channels and for voluntary cooperation.<br>+ Streamlining of procedures and standards could increase effectiveness of voluntary cooperation channels.<br>+ Increase in total number of requests because requests that were not done previously because of the complexity/ lack of knowledge about the procedure would now be done, i.e. more evidence available for investigations and prosecutions.<br>- Effectiveness of measures will depend on willingness to implement them.<br>+ The platform and form to exchange EIO requests will allow public authorities to secure and obtain e-evidence more quickly and effectively, whilst fulfilling the necessary security requirements;<br>+ The platform would enable better collection of statistics, indicators and evaluation of the instrument.<br>- EIO's scope is limited to EU territory, and will not cover | **-1** |

| | | |
|---|---|---|
| | service providers headquartered in non-EU countries, nor in Ireland and Denmark.<br><br>International solutions can bring some improvements to the shortcomings of the legal framework, depending on what is agreed.<br><br><u>Budapest</u><br>+ A multilateral solution in the framework of the Budapest Convention (Additional Protocol) would have a broad geographical scope and could possibly also include the US.<br>+/- The large group of parties of the Budapest Convention is an advantage and a disadvantage in this context. It is an advantage insofar as any common solution applies to a large number of partner countries of the EU. The downside of the large number of parties lies in the smaller common denominator that exists across a diverse group such as this one. This may create a risk for the drafting process and may also result in a reduced scope of any such protocol. In any case, it appears evident that the new protocol, while certainly helpful beyond the EU, would not be able to match the level of integration within the EU because of a lack of a common and harmonised framework of safeguards across all the countries that are party to the Budapest Convention.<br>The potential effectiveness is however difficult to assess, as it will depend on provisions negotiated and participating states. Negotiations would be long.<br><br><u>Bilateral agreements</u><br>+ Bilateral agreements would create more legal certainty on the basis and process for cooperation with private parties in non-EU countries.<br>++ Bilateral EU-US agreements would allow US service providers to provide content data.<br>- Bi- or multilateral agreements are uncertain; it could take years, if at all, to reach an agreement, be it on a multilateral agreement or on a bilateral one, and it would depend on the non-EU countries involved.<br><br>- The issue linked to access to the WHOIS database would not be solved | |
| **Efficiency** | - Administrative costs would be incurred by public authorities and service providers for implementing practical measures.<br>+ Practical measures may lead to a slight shift from judicial cooperation channels to direct cooperation channels, generating savings.<br>+ Carrying out the measures would improve the quality of requests, leading to a reduction in resources for both public and private entities. | **+0,5** |

| | | |
|---|---|---|
| | + SPOC system and standardised procedures could reduce burden on service providers and public authorities.<br>EIO platform and form:<br>- Initial increase to baseline costs for EU budget and Member States in developing and connecting to the secure online secure platform.<br>++ Once platform is up and running, costs will be reduced compared to the baseline.<br>- Member States public authorities will incur some costs in disseminating the electronic form to their judicial authorities, if it is already used before the platform is up and running.<br>+ International solutions allowing direct cooperation with service providers would have similar advantages for businesses and for public authorities as legislative measures on direct cooperation detailed below. | |
| **Competitiveness** | + With international agreements, whether bilateral or multilateral, legal certainty would be improved and conflicts of law avoided in relation to the states that are party to the agreement. | **0** |
| **Fundamental rights and freedoms** | Impact on fundamental righst stems from international measures only:<br>+ International agreements may be advantageous in terms of ensuring an adequate level of protection of fundamental rights, including data protection. They could allow to ensure appropriate level of fundamental rights protection comparable to that of the EU-internal solution. Given wider geographical coverage, they could have added value compared to other options.<br>- It is debatable, however, whether the same level of fundamental rights protection would be ensured by a multirateral solution compared to a bilateral one, given a broader geographical approach and thus more varying levels of safeguards in different countries.<br>0 The (draft) Terms of Reference for the Preparation of a the Additional Protocol to the Budapest Convention on Cybercrime contain a mandate to prepare text on safeguards (including data protection requirements) for cross-border access to information. It is too early to assess the level of fundamental rights protection that would be achieved by the Additional Protocol.<br>- In the framework of bilateral agreements such as with the US, it would most likely be easier to negotiate an adequate level of fundamental rights protection.<br>+ Regarding data protection, the Umbrella Agreement would apply to an EU-US agreement, ensuring a high level of protection. | **+2** |
| **Impact on 3rd countries and international** | (+)Training of EU practitioners in US law requirements will reduce costs also for US authorities involved in MLA procedures | **+2** |

| | | |
|---|---|---|
| **relations** | + By ensuring mutual understanding on conditions for direct cooperation with service providers, with a wide geographical scope, this option offers considerable advantages on the potential issues of extra-territoriality (intrusion on the sovereignty of another country).<br>+ International agreements could allow for a joint definition of mutually acceptable conditions, thus reducing conflicts of law.<br>+ International agreements, in particular multirateral ones, would reduce to a minimum the risk of reciprocal responces from non-EU countries, even if they would never cover all states worlwide. | |

**Option C: Option B + direct cooperation legislation (access to databases + EPO)**

| Criteria | Assessment | Score |
|---|---|---|
| **Effectiveness/ social impact** | A combination of all measures proposed, excluding a measure on direct access, would bring important gains in terms of improving the capacity of public authorities to investigate and prosecute crimes. It would allow combining the benefits described above for 6 measures (based on measure 5), as the options are complementary.<br>The legislative measure on EPO would bring significant improvements;<br><br>+++A significant shift from judicial cooperation channels to the European Production Order can be expected, which would make access to e-evidence faster and more efficient. This concerns predominantly intra-EU requests, as direct cooperation was previously not possible here. A significant change in numbers regarding direct cooperation with US providers is not expected, but for other third-country providers which offer services in the EU, this could also take pressure off the MLA channels. In addition, public authorities will attempt to obtain such data also in cases where today they may have been discouraged even to try due to the cumbersome procedure required. As a result, an increase in the total number of direct cooperation requests being issued by public authorities could therefore be expected.<br>+ Improvements of judicial cooperation channels will still be useful: where the EPO would not help, e.g. in conflicts of law situations (content data with the US), judicial cooperation will prevail. For judicial cooperation among Member States, EIOs may still be issued to obtain e-evidence, even where direct cooperation provides for a faster access, e.g. when an investigating State needs different types of evidence from another Member State at the same time. | **+2,5** |

| | | |
|---|---|---|
| | ++ Legislation providing for a legal basis to perform searches in the WHOIS database would enable authorities to continue to access the system in much the same manner as they currently do, even if some of its data elements should become password-protected and no longer publicly available. Authorities specialised in cybercrime make look-ups to the WHOIS many times a day. Providing a new legal basis for the changed circumstances would preserve an essential tool in online investigations and would prevent a significant decrease in effectiveness of investigations.<br>- However, issues to access data directly would not be addressed and would therefore likely remain, unless an international solution is found in the context of the additional protocol to the Budapest Convention. - + Some of the practical measures to improve cooperation between public authorities and service providers would to some extent become superfluous once a legislative measure on EPO or EPR comes into force, as the legislation would establish a procedure, standard forms and an obligation to designate a legal representative. As this may still take many years, there would still be a benefit in the short term from introducing these practical measures on a voluntary basis.<br>+++ The international solutions would complement legislative measures. In particular, once an agreement with the US would be in place, the measure on cooperation with service providers would also allow public authorities to obtain access to content data, as the conflict would no longer exist.<br>- However, international solutions remain uncertain and long-term. | |
| **Efficiency** | +++ A combination of 6 measures would result in cumulated cost reductions for both service providers and public authorities compared to the baseline scenario. The expected significant shift from judicial cooperation channels to cooperation with service providers (see above under Effectiveness) would lead to important cost savings for judicial authorities both in the issuing and in the receiving State. Improvements in judicial cooperation channels, which would remain relevant in certain cases, would also result in some cost savings. Implementation of both practical and legislative measure would generate some costs for Member States, but these would probably be offset by the cost savings described above.<br>- The biggest change for service providers is that they would receive more requests directly from public authorities in another Member State, rather than from their own public authorities via MLA or EIO channels.<br>+ The main benefit for them would be the legal certainty and the harmonisation of procedures and forms of requests. | **+1,5** |

| | | |
|---|---|---|
| | ++ If a solution is provided for access to WHOIS, authorities might be able to maintain the level of access they benefit from today, as the databases concerned are already in place. Therefore, costs would remain the same; there would be no additional costs generated by this proposal on the providers' side, and the same would be true for authorities. Costs generated by the planned changes to the WHOIS database system are independent of this proposal. The proposal would also prevent an avalanche of individual orders to service providers to produce the data, which might otherwise generate significant costs for both sides. | |
| **Competitiveness** | + Improved legal certainty deriving from legislation on EPO and from international agreements will benefit service providers. Clear obligations on their side will no longer make it necessary to assess legality of requests for data.<br>- Improved access by EU authorities to e-evidence could affect business models chosen by service providers, in particular where data location and access to this data is an important factor for customers. This is specifically the case for some corporate clients. This would be mitigated by a "controller first" principle. | **-1,5** |
| **Fundamental rights and freedoms** | When assessing a combination of all measures, the main measure impacting fundamental rights is the legislative measure on a European Production Order. The measure would create a legal framework including sufficient safeguards to make it compatible with fundamental rights.<br>On the other hand, by not including a measure on direct access, or delaying its adoption, option C would leave the direct access to diverging national regimes, thereby not ensuring a similar high level of protection in the Union of direct access measures; safeguards would remain a national issue. Minimum safeguards could potentially stem from the additional protocol to the Budapest Convention, but it is too early to say. With a functioning mechanism to obtain data from service providers, it can be assumed that there would be fewer incentives for Member States to use direct access also in situations where they could instead go to a service provider. | **+1** |
| **Impact on 3rd countries and international relations** | The main impact on non-EU countries stems from extraterritorial effects of the legislative measure on a European Production Order, even if steps are taken to mitigate those, notably with the conflicts of law clause.<br>If these measures are combined with international solutions, for which they could serve as a source of inspiration, this would greatly contribute to achieving acceptance of these measures. | **+1** |

**Option D: option C + direct access**

| Criteria | Assessment | Score |
|---|---|---|
| **Effectiveness/ social impact** | A combination of all measures proposed would bring the biggest gain in terms of improving the capacity of public authorities to investigate and prosecute crimes. It would allow combining the benefits described above for all 7 measures (based on measure 5), as the options are complementary.<br>+++ The two legislative measures address different situations and would, if combined, provide for a set of efficient tools to obtain cross-border access to e-evidence. The option to provide a legal basis for Member States to adopt legislation on direct access, subject to stringent conditions and safeguards, could improve the capacity of public authorities to investigate and prosecute crimes, both with regard to the time to obtain data and to the number of cases where e-evidence is successfully obtained.<br>+++A shift from judicial cooperation channels to these two tools can be expected, which would make access to e-evidence faster and more efficient. Improvements of judicial cooperation channels will still be useful: where the EPO would not help, e.g. in conflicts of law situations (content data with the US), judicial cooperation will prevail. For judicial cooperation among Member States, EIOs may still be issued to obtain e-evidence, even where direct cooperation provides for a faster access, e.g. when an investigating State needs different types of evidence from another Member State at the same time.<br>++ Legislation providing for a legal basis to perform searches in the WHOIS database would enable authorities to continue to access the system in much the same manner as they currently do (see above Option B).<br>- Some of the practical measures to improve cooperation between public authorities and service providers would to some extent become superfluous once a legislative measure on EPO or EPR comes into force, as the legislation would establish a procedure, standard forms and an obligation to designate a legal representative. As this may still take many years, there would still be a benefit in the short term from introducing these practical measures on a voluntary basis.<br>+++ The international solutions would complement legislative measures. In particular, once an agreement with the US would be in place, the measure on cooperation with service providers would also allow public authorities to obtain access to content data, as the conflict would no longer exist.<br>- However, international solutions remain uncertain and long-term. | **+3** |

| | | |
|---|---|---|
| **Efficiency** | +++A combination of all 7 measures would result in cumulated cost reductions for both service providers and public authorities compared to the baseline scenario. The expected shift from judicial cooperation channels to cooperation with service providers and, to a lesser extent, to direct access, would lead to important cost savings for judicial authorities both in the issuing and in the receiving State. Improvements in judicial cooperation channels, which would remain relevant in certain cases, would also result in some cost savings. Implementation of both practical and legislative measure would generate some costs for Member States, but these would probably be offset by the cost savings described above.<br>- The biggest change for service providers is that they would receive more requests directly from public authorities in another Member State, rather than from their own public authorities via MLA or EIO channels.<br>+ The main benefit for them would be the legal certainty and the harmonisation of procedures and forms of requests. | **+2** |
| **Competitiveness** | + Improved legal certainty deriving from legislation on EPO and from international agreements will benefit service providers. Clear obligations on their side will no longer make it necessary to assess legality of requests for data.<br>- Improved access by EU authorities to e-evidence could affect business models chosen by service providers, in particular where data location and access to this data is an important factor for customers. This is specifically the case for some corporate clients. This would be mitigated by a "controller first" principle. | **-1,5** |
| **Fundamental rights and freedoms** | When assessing a combination of all measures, the main options impacting fundamental rights are the two legislative measures. The two measures would create a legal framework including sufficient safeguards to make the measures compatible with fundamental rights.<br>A combination of all legislative measures, including international solutions, would facilitate cross-border access to personal data to the biggest extent, but would also ensure that fundamental rights are most widely protected in all situations covered by these measures. If only some of these measures would be pursued by Union law, it would still leave room for either national unilateral solutions and/or voluntary cooperation outside of a clear legal framework. The legislative measures would also ensure that the practical measures can take place in a legal framework where fundamental rights are protected, thereby complementing the practical measures from a fundamental rights point of view. | **+1** |
| **Impact on 3rd countries and international relations** | The main impact on non-EU countries stems from extraterritorial effects of the two legislative measures, even if steps are taken to mitigate those, notably for the EPO with the conflicts of law clause. The risk of reciprocal | **+0,5** |

| | | |
|---|---|---|
| | responses for a measure on direct access is more difficult to mitigate.<br>If these measures are combined with international solutions, for which they could serve as a source of inspiration, this would greatly contribute to achieving acceptance of these measures. | |

## 3. Quantitative assessment of policy measures

This section describes how the model to calculate the costs works, the assumptions used and the limitations.

### 1. How the model works.

As described in section 6.2., the model calculates the **administrative costs** for the 2 groups of stakeholders which would incur in costs in this initiative: **public authorities** and **service providers**. These costs have two components: the salary/minute and the minutes it takes to do the tasks:

| Costs = **cost/minute** of the person doing the tasks x **minutes** required to do the tasks |
|---|

- **Cost/minute**:
  - It includes:
    - the salary, based on the median of the salaries in the EU of the level 2 workers (professionals) in the International Standard Classification of Occupations (ISCO)[184];
    - non-wage labour costs such as employers' social contributions;
    - 25% overhead (i.e. expenses not related to direct labour, such as the cost of office equipment.)
  - The value is **30 EUR/hour = 50 cents/minute**.
- **Minutes** required to do a task:
  - Since the salary/minute is assumed constant, the model focuses on estimating the minutes required to do the tasks.
  - This minutes required to do the tasks can change if:
    - the **time** required to do **one task** changes, or
    - the **total number of tasks** changes.

The **one-off costs** were calculated using estimates on the time it takes to carry out the tasks (e.g. transposition of legislation), from comparable situations.

The **continuous costs** were calculated in comparison with the baseline:

[184] Based on 2014 Mean Hourly Earnings By Main Economic Activity And Occupation* + adjustment to 2014 Prices. No data for Croatia was available. Source: Eurostat, Structure of Earnings Survey - NACE Revision 2.

1. First, the costs of the baseline were calculated, including the time/attempt and the number of attempts to access e-evidence across borders in each of the channels (judicial cooperation, direct cooperation and direct access) and for both public authorities and service providers.
2. Second, it was estimated how each of the options changed the time/attempt and the number of attempts in each of the channels and stakeholders group in relation to the baseline (% of deviation from the baseline parameters). These group of percentages are called "modifiers" in the explanations below are tabled for each of the options.
3. Finally, the continuous costs for that option resulted from applying the modifiers to the baseline values to obtain the time/attempt and the number of attempts for each option's scenario.

In summary, to calculate the costs of each option, the following questions were analysed for each of the measures:

1. Are there any **one-off costs**? (e.g. initial costs to set a system of contact points).
2. Does the measure **change** any of the **times** required to do **any task** required to attempt to access e-evidence across borders in **each of the three channels** (i.e. judicial cooperation, direct cooperation and direct access)?
3. Does the measure **change** the **total number** of **attempts** to access e-evidence across borders in **each of the 3 channels**?
4. Combining the above, does the measure **change** the **total time** to attempt to access e-evidence across borders?
5. Combining the above, does the measure **change** the **total continuous costs** to attempt to access e-evidence across borders?

The following **general assumptions** were made:

- The cost/minute = 30 EUR/hour = 50 cents/minute remains **constant** for all options and over time.
- The time required to do a task is the **average** of **content and non-content** requests as well as of **intra-EU** requests and requests involving **non-EU** countries.
- **Continuous costs for preservation orders** were not included in the calculation since the impact of a possible measure on preservation was deemed to be negligible: a procedure for preservation already exists both in judicial and direct cooperation and would simply be put on more secure legal footing. In terms of the actual procedures and requirements, there would be no change. The (comparatively small) cost of implementing legislation on preservation orders is included in the one-off costs for implementation of the European Production Order, which a preservation order could complement.

The next section describes the **specific assumptions** used to answer the above questions for each of the options.

## 2. Calculation of the cost estimates for each options: assumptions.

Measure 0: baseline

The analysis of the costs of the baseline serves as a reference to estimate the costs for public authorities and service providers of the other options.

1) One-off costs.
   There are logically no one-off costs in the baseline.

2) Time per attempt per channel.
   For judicial and direct cooperation, the data to calculate the time per attempt was obtained through targeted surveys 3 and 4 to public authorities and service providers respectively (see Annex 2).

   The following tasks were considered for each channel and stakeholder, for subscriber data, metadata and content data:
   - Judicial cooperation:
     - Issuing authorities:
       - Obtain a national judicial decision/warrant to request data.
       - Fill in the request form.
       - Ask for validation by a judicial authority.
       - Identify the competent authority to receive the request for data in the executing State.
       - Submit the request for data to the competent authority of the executing State.
       - Monitor that evidence/refusal to provide the requested data was received.
       - Reply to requests for consultation/additional information from the executing State.
       - Amend/withdraw the request for data.
     - Executing authorities:
       - Verify request and assess grounds for refusals
       - Ask for authorisation by a court
       - Submit the request to the relevant service provider
       - Monitor that a reply was received
       - Enforce if no request is received (by setting fine or by other means)
       - Verify grounds for refusal relating to immunities and privileges, once data is received from service provider

        - Transmit data to issuing authority.

    When the executing/requested authority is outside of the EU, the administrative costs were not counted.

    The estimates for the issuing authority was obtained through the targeted survey on costs to public authorities. It was estimated that it takes the executing authority **half** the time to perform its tasks compared to the issuing authority.

    - Service providers:
        - Legal review of one request for data (appropriateness and authenticity of the order).
        - Initial processing and validation of one request for data.
        - Contact the EU authority for further clarifications when needed.
        - Send out a notification to the user.
        - Retrieve relevant information from existing data.
        - Hold internal or external meetings (e.g. with lawyers).
        - Fill in tables and forms.
        - Data transformation (converting data to required format).
        - Submit the information to the issuing EU authority.
        - Prepare cost reimbursement request (where applicable).
        - Oversee the full process of processing one request for data.
- Direct cooperation:
    - Public authorities:
        - Identify the digital service provider that holds the requested data.
        - Fill in the legal request form.
        - Language translation of one request for data.
        - Submit the legal request form to the identified digital service provider.
        - Receive the requested data.
        - Contact the digital service provider for further clarifications when needed.
        - Verify the authenticity and integrity of the received data from the digital service provider.
        - Language translation of received data.
        - Data transformation (converting data to required format).
        - Send out a notification to the user.
        - Oversee the full process of processing legal request.
        - Monitor that no reply was received.
    - Service providers:
        - Idem tasks for judicial cooperation.

- Direct access:
    - There was no data available for the time per attempt for public authorities in direct access and none was obtained through the targeted surveys.
    - It was estimated at **20%** of the time required for judicial cooperation, since:
        - Regarding judicial oversight, what is needed here is a national judicial authorisation, which is obtained much faster than a full judicial cooperation procedure involving a second state.
        - The judicial authorisation required for the search warrant to obtain the device that would for extended search or the judicial authorisation to obtain the credentials that allow for remote access is part of the larger investigation, not necessarily an exclusive task of cross-border access to e-evidence.

3) Total number of attempts per channel.
    - Judicial cooperation:
        - Intra-EU MLA/EIO requests were estimated at **13,000/year**, using data from Eurojust and the European Judicial Network (see section 2 on the size of the problem).
        - MLA requests with non-EU countries were estimated at **1,300/year**, using data from the US Department of Justice and the EU-US MLA Review report of 2015 (see section 2 on the size of the problem). MLA requests to other non-EU countries other than the US were considered negligible.
        - The growth rate of the above requests (both intra EU and with non-EU countries) was assumed to be **14%**, the same as the CAGR of the direct cooperation requests in the 2013-2016 period obtained from the transparency reports (see below).
        - It was assumed that the expected reduction in the availability for law enforcement to consult the **WHOIS database** would result in a **doubling** of the judicial cooperation requests from 2018 onwards. This is a conservative estimate, as numbers of WHOIS look-ups is estimated to be much more important than the number of judicial cooperation requests. On the other hand, it is unlikely that public authorities would replace every single look-up by a judicial cooperation request, given the resources that would need to be deployed.
        - Since the purpose is to calculate the continuous costs per year, the model used an average number of total attempts per year, calculated over a 10 year period (i.e. total estimated number of attempts in the

2017-2026 period divided by 10, considering an annual growth of 14%, equal to the CAGR of the number of direct cooperation requests in the 2013-2016 period, as described in section 2.1.1.), resulting in **61,417** requests.

- Direct cooperation:
  - The estimated total number of requests in 2016 was **120,000**, taken from the transparency reports of the main 5 service providers (Google, Facebook, Microsoft, Apple and Twitter), as shown in section 2 (size of the problem part).
  - The annual growth in the number of requests was assumed to be the same as the CAGR in the 2013-2016 period, **14%** (see section 2).
  - Considering the above, the average number of direct cooperation requests in the 2017-2026 period is **264,534.**
- Direct access:
  - Practitioners indicated that the number of direct access attempts was about equal (i.e. 100%) to the number of judicial cooperation requests, since:
    - Direct access is a relatively fast and therefore efficient tool; practitioners stated that they had increasingly resorted to direct access over the past years in the face of inefficient direct or judicial cooperation.
    - On the other hand, it is still used much less than direct cooperation, as it requires specific circumstances when a search can be ordered, i.e. there must already be sufficient evidence against a person, and there are legal requirements to be fulfilled because of the intrusiveness of the measure.
    - Direct access furthermore requires that authorities have access either to the device or to credentials, which is the case in much fewer situations as compared to requests to providers.

4) Total time.
   It was calculated as the product of the time/attempt and the number of attempts, for each of the channels and both groups of stakeholders (public authorities and service providers).

5) Total continuous costs.
   It was calculated as the product of the total time and the salary of 50 cents/minute indicated above.

The table below summarises the calculations of the continuous costs per year for the baseline[185]:

| | Judicial cooperation | | Direct cooperation | | Direct access | Total per year |
|---|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities | |
| Time/attempt (min) | 321 | 146 | 118 | 146 | 64 | |
| Attempts | 61,417 | | 264,534 | | 61,417 | **387,368** |
| Total time (min) | 19,714,895 | 8,966,899 | 31,215,035 | 38,621,993 | 3,942,979 | **102,461,801** |
| | | | | | ***Total continuous costs per year*** | ***€ 51,230,900*** |

Measure 1: practical measures to enhance judicial cooperation

1) One-off costs.
   The one-off costs in this measure concern the costs for Member States of joining the secure online platform for enhancing judicial cooperation within the EU.

   The one-off costs are **400,000 EUR**, which correspond to: installation, configuration and testing of e-CODEX + reference e-Evidence Portal for 16 participating Member States (AT, HR, IT, NL, GR, PT, NL, FR, IT, LU, LT, EL, BG, CZ, ES, DE) at 25,000 EUR per Member State (the rest, 80% of the total cost, will be funded by the European Commission through grants).

2) Time per attempt per channel.
   - Judicial cooperation:
     - Public authorities: **-10%** in relation to the baseline.
       - Increased efficiency thanks to the improvements introduced by the practical measures.
       - Higher quality of requests due to training for practitioners, meaning less back and forth between the two authorities.
       - Swifter transmission channels intra-EU thanks to platform.
       - On the other hand, the cooperation mechanism itself remains unchanged, which limits the possible impact that can be achieved.
     - Service providers: **0%** in relation to the baseline.
       - No impact on service providers since receiving authority acts as filter when requests are of bad quality.
   - Direct cooperation:

[185] These figures represent averages. It should also be noted that according to feedback received from big service providers, 80-90% of all attempts are routine cases that take less time than indicated thanks to efficient procedures put in place by big service providers, but the statistics are influenced by the remaining number of problematic cases that take much longer.

- Public authorities: **0%** in relation to the baseline.
    - No impact since these measures concern enhancement of judicial cooperation.
- Service providers: **0%** in relation to the baseline.
    - No impact since these measures concern enhancement of judicial cooperation.

- Direct access:
  - Public authorities: **0%** in relation to the baseline.
    - No impact since these measures concern enhancement of judicial cooperation.

3) Total number of attempts per channel.
   - Judicial cooperation:
     - Public authorities: +**10%** in relation to the baseline.
       - With improved know-how due to training and information being more easily available, more requests can be expected to be made, both due to authorities being able to use known channels more effectively and due to authorities learning about the possibility to use these channels for their cases.
       - Some of the direct cooperation requests would be made through judicial cooperation instead.
     - Service providers: **+10%** in relation to the baseline.
       - Idem public authorities.
       - The % change is in relation with the number of attempts in the baseline.
   - Direct cooperation:
     - Public authorities: **-0%** in relation to the baseline.
       - The increase in efficiency in judicial cooperation could slightly decrease the number of direct cooperation requests, but this effect would likely be negligible.
     - Service providers: 0**%** in relation to the baseline.
       - There would only be a negligible impact on service providers, public authorities act as filters..
   - Direct access:
     - Public authorities: **0%** in relation to the baseline.
       - No impact since these measures concern enhancement of judicial cooperation.

The table below summarises the above modifiers for this measure:

| | Judicial cooperation | | Direct cooperation | | Direct access |
|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities |
| Time/attempt (min) | -10% | 0% | 0% | 0% | 0% |
| Attempts | 10% | | 0% | | 0% |

4) Total time.
   It was automatically calculated using the above assumptions following the same reasoning as in the baseline.

5) Total continuous costs.
   It was automatically calculated using the above assumptions following the same reasoning as in the baseline.

The table below summarises the total continuous costs per year for this measure:

| | Judicial cooperation | | Direct cooperation | | Direct access | Total per year |
|---|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities | |
| Time/attempt (min) | 289 | 146 | 118 | 146 | 64 | |
| Attempts | 67,559 | | 264,534 | | 61,417 | **393,510** |
| Total time (min) | 19,517,746 | 9,863,589 | 31,215,035 | 38,621,993 | 3,942,979 | **103,161,341** |
| | | | | | ***Total continuous costs per year*** | ***€ 51,580,671*** |

Measure 2: practical measures to enhance direct cooperation

1) One-off costs.
   - Public authorities:
     - Set up the SPOC system:
       - 30 working days x 22 Member States without SPOC (all except FR, UK, SE, BE, FI, LT).
       - The setting up of a SPOC system requires conceiving, validating and implementing such system for the whole Member State, involving various actors and levels of validation. Persons working as (part of) the SPOC need to be trained.
       - Costs may differ largely depending on what kind of SPOC system is established, 30 working days would represent an average figure
     - Standardise procedures:
       - 20 working days x 28 Member States.
       - Standardising procedures should be slightly faster than setting up SPOCS, as it does not require a new structure to be created.
       - Nonetheless it would require a significant amount of effort, which could vary across Member States depending on the number of

different authorities that participate, the number of existing procedures, and the internal resistance to change.
        - This estimate would include the time for assessment of existing procedures, development of a streamlined and simplified process, and implementation of that process.
        - This would likely be facilitated by the existence of a SPOC and could take additional time if no SPOC is put in place.

- Service providers:
    - Set up the SPOC system:
        - 20 working days x top 10 service providers.
        - As this is a voluntary measure, it was estimated that only the service providers receiving large volumes of requests already would see it proportionate to invest in it. Furthermore, this is only an option for US-based service providers given the legislation in place.
        - 10 service providers is an estimate on the high side, as a number of the top service providers have already put into place SPOCs or functionally equivalent systems.
        - The setting up of SPOC should be slightly faster for service providers, as it would not involve as many actors and the validation process may be less formal. Furthermore, many service providers already have some or all of the SPOC process implemented and would not need to start from zero if they choose to implement this.
        - Persons working as SPOC need to be trained.
        - Costs may differ largely depending on what kind of SPOC system is established, 20 working days would represent an average figure
    - Standardise procedures:
        - 30 working days x top 10 service providers.
        - This estimate includes internal assessments of procedures currently in place; time spent discussing with other service providers what could be streamlined; designing standardised procedures; and then time is still required to implement the measures decided. It is estimated to require more efforts than setting up a SPOC, which is a purely internal measure, while this requires agreement across several service providers.
        - As this is a voluntary measure, it was estimated that only the service providers receiving large volumes of requests already would see it proportionate to invest in it. Furthermore, this is only

an option for US-based service providers given the legislation in place.

2) Time per attempt per channel.
   - Judicial cooperation:
     - Public authorities: **0%** in relation to the baseline.
       - No impact since these measures concern enhancement of direct cooperation.
     - Service providers: **0%** in relation to the baseline.
       - No impact since these measures concern enhancement of direct cooperation.
   - Direct cooperation:
     - Public authorities: **-15%** in relation to the baseline.
       - Increased efficiency thanks to the improvements introduced by the practical measures.
       - Improvements through practical measures for direct cooperation are expected to have a slightly bigger impact than the practical measures on judicial cooperation, as they will be more numerous and will modify how this channel works; the setting-up of SPOCs and streamlining of procedures is expected to have most impact.
     - Service providers: **-15%** in relation to the baseline.
       - Increased efficiency thanks to the improvements introduced by the practical measures.
       - Quality of requests is expected to improve, reducing the need for back-and-forth; number of requests that service providers do not answer under their individual policy would be expected to decrease.
   - Direct access:
     - Public authorities: **0%** in relation to the baseline.
       - No impact since these measures concern enhancement of judicial cooperation.

3) Total number of attempts per channel.
   - Judicial cooperation:
     - Public authorities: -5**%** in relation to the baseline.
       - The increase in efficiency in direct cooperation would lead to a shift from judicial cooperation requests to direct cooperation requests.
       - Training and SPOCs would help practitioners understand better in which situations they can resort to direct cooperation.
       - The SPOC system might help redirect requests to direct cooperation where appropriate.
     - Service providers: **-5%** in relation to the baseline.
       - Idem public authorities.

        - The % change is in relation with the number of attempts in the baseline.
- Direct cooperation:
    - Public authorities: +10**%** in relation to the baseline.
        - The efficiency improvements would facilitate adding new requests that before were not done due to the complexity of the process or the lack of knowledge about the procedure to follow for a particular service provider.
        - Some of the judicial cooperation requests would be done through direct cooperation.
    - Service providers: **+10%** in relation to the baseline.
        - Idem public authorities.
        - The % change is in relation with the number of attempts in the baseline.
- Direct access:
    - Public authorities: **0%** in relation to the baseline.
        - No impact since these measures concern enhancement of judicial cooperation.

The table below summarises the above modifiers for this measure:

| | Judicial cooperation | | Direct cooperation | | Direct access |
|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities |
| Time/attempt (min) | 0% | 0% | -15% | -15% | 0% |
| Attempts | -5% | | 10% | | 0% |

4) Total time.
   It was automatically calculated using the above assumptions following the same reasoning as in the baseline.

5) Total continuous costs.
   It was automatically calculated using the above assumptions following the same reasoning as in the baseline.

The table below summarises the total continuous costs per year for this measure:

| | Judicial cooperation | | Direct cooperation | | Direct access | Total per year |
|---|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities | |
| Time/attempt (min) | 321 | 146 | 100 | 124 | 64 | |
| Attempts | 58,346 | | 290,988 | | 61,417 | **410,751** |
| Total time (min) | 18,729,150 | 8,518,554 | 29,186,058 | 36,111,563 | 3,942,979 | **96,488,304** |
| | | | | | ***Total continuous costs per year*** | ***€ 48,244,152*** |

Measure 3: multilateral international agreements

It is not possible to quantify the costs that this measure would generate since the agreements have not been negotiated yet.

Measure 4: bilateral international agreements

It is not possible to quantify the costs that this measure would generate since the agreements have not been negotiated yet.

Measure 5: European Production Order

1) One-off costs.
   - Public authorities:
     - Transpose EU legislation:
       - 200 working days x 27 Member States: time of 200 working days based on a previous Commission study[186]. Assumes all Member States would take part, except DK.
       - Assumes that the instrument would be a directive. If the instrument were a regulation it would not require transposition, but still some adaptations of national law to make it compliant with the instrument.
   - Service providers:
     - Set up the legal representative:
       - 30 working days X 130 service providers
       - Setting up a legal representative would mean to designate a legal or natural person in the Union; if no establishment is available, it would require negotiating contractual arrangement with a third person who could act as legal representative; liability for sanctions will also have to be taken into Account. The number of 130 service providers is based on feedback from Member States' authorities as to the number of providers they regularly make requests to.
       - This may require comparatively more efforts than setting up a SPOC, which is an internal procedure.
       - Cost savings may result from an accumulation of functions with an (already established) GDPR representative.
       - For service providers within the EU, the nomination is assumed to require less efforts.

[186] Study for an impact assessment on a proposal for a new legal framework on identity theft, 2012, p160.

- Adapt operating procedures and contractual framework:
  - 20 working days X 130 service providers
  - In parallel to the designation of the legal representative, internal processes have to be put in place so that the data is provided within the deadline to the legal representative

2) Time per attempt per channel.

- Judicial cooperation:
  - Public authorities: **0%** in relation to the baseline.
    - No impact since this measure does not affect judicial cooperation times.
  - Service providers: **0%** in relation to the baseline.
    - No impact since this measure does not affect judicial cooperation times.
- Direct cooperation:
  - Public authorities: +**10%** in relation to the baseline.
    - Time spent per request is expected to increase because additional duties are added (collection of statistics).
    - The additional time required for judicial review, user notification and collecting statistics would be partially offset by the streamlining of procedures.
    - There would be one procedure applicable to all service providers covered by the scope of the instrument.
  - Service providers: **-5%** in relation to the baseline.
    - Increased efficiency thanks to the harmonised legal framework, reducing efforts to assess the legitimacy of requests. Additional time may result from the use of the legal representative and the assessment of conflicting obligations.
    - However, the additional time required for conflict of laws and legal representative would be offset by the increase in efficiency and legal certainty of having one legal framework and mandatory measures.
    - Where service providers use a third-party legal representative, they may incur ongoing costs to maintain the representative relationship.
    - The main gains are likely to occur in service providers' relationship with countries currently issuing a lower number of requests than with countries issuing a higher number of requests and which already have more efficient procedures in place.

- Direct access:
  - Public authorities: **0%** in relation to the baseline.
    - No impact since this measure does not affect direct access times.

3) Total number of attempts per channel.
   - Judicial cooperation:
     - Public authorities: -40**%** in relation to the baseline.
       - A significant number of the judicial cooperation requests in the EU would transfer to EPO. Less change for data held by US service providers: For US requests, most of the content requests would be subject to conflicts of law until there is an international agreement, which means this type of evidence would remain under judicial cooperation channels.
       - For non-content data held by US providers, direct cooperation is already possible even if not comprehensively regulated, reliable or legally certain.
     - Service providers: -40**%** in relation to the baseline.
       - Idem public authorities.
       - The % change is in relation with the number of attempts in the baseline.
   - Direct cooperation:
     - Public authorities: +10**%** in relation to the baseline.
       - Some of the judicial cooperation requests would be made through direct cooperation – see above – in particular within the EU.
       - In addition, authorities might now make some requests through direct cooperation that they previously did not make through judicial cooperation, given the administrative burden.
       - Because the volume of direct cooperation requests is already much more important than the volume of judicial cooperation requests, the percentage growth is much lower than for judicial cooperation.
       - No comparable shift is expected with the US as the majority of requests already goes through direct cooperation. While the overall volume would not rise significantly in that context, the quality of requests would change as the requests move from voluntary to obligatory. Additional providers who currently do not participate in voluntary cooperation would be added.
     - Service providers: **+10%** in relation to the baseline.
       - Idem public authorities.
       - The % change is in relation with the number of attempts in the baseline.
   - Direct access:
     - Public authorities: **-5%** in relation to the baseline.
       - Relatively small decrease in the number of direct access attempts as direct cooperation becomes more effective and some of the attempts shift back to direct cooperation.

The table below summarises the above modifiers for this measure:

| | Judicial cooperation | | Direct cooperation | | Direct access |
|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities |
| Time/attempt (min) | 0% | 0% | 10% | -5% | 0% |
| Attempts | -40% | | 10% | | -5% |

4) Total time.
   It was automatically calculated using the above assumptions following the same reasoning as in the baseline.

5) Total continuous costs.
   It was automatically calculated using the above assumptions following the same reasoning as in the baseline.

The table below summarises the total continuous costs per year for this measure:

| | Judicial cooperation | | Direct cooperation | | Direct access | Total per year |
|---|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities | |
| Time/attempt (min) | 321 | 146 | 130 | 139 | 64 | |
| Attempts | 36,850 | | 290,988 | | 58,346 | **386,184** |
| Total time (min) | 11,828,937 | 5,380,139 | 37,770,193 | 40,359,982 | 3,745,830 | **99,085,081** |
| | | | | | ***Total continuous costs per year*** | ***€ 49,542,541*** |

Measure 6: access to data without individualised review

1) One-off costs.
   - Public authorities:
     - Transpose EU legislation:
       - 100 working days x 27 Member States: time of 100 working days based on a previous Commission study[187]. Assumes all Member States would take part, except DK.
       - Assumes that the instrument would be a directive. If the instrument were a regulation it would not require transposition.
2) Time per attempt per channel.
   - Judicial cooperation:
     - Public authorities: **0%** in relation to the baseline.

[187] Study for an impact assessment on a proposal for a new legal framework on identity theft, 2012, p160.

        - No impact since this measure does not affect judicial cooperation times.
    - Service providers: **0%** in relation to the baseline.
        - No impact since this measure does not affect judicial cooperation times.
- Direct cooperation:
    - Public authorities: **0%** in relation to the baseline.
        - No impact since this measure does not affect the direct cooperation times from the public authorities perspective.
    - Service providers: **0%** in relation to the baseline.
        - No impact on time it takes to process direct cooperation requests.

- Direct access:
    - Public authorities: **0%** in relation to the baseline.
        - No impact since this measure does not affect direct access times.

3) Total number of attempts per channel.
    - Judicial cooperation:
        - Public authorities: **-50%** in relation to the baseline.
            - Transfer of requests from judicial cooperation to direct cooperation, since public authorities would be able to access directly the Whois databases instead of making individualised requests to service providers.
            - A complete transfer is to be expected as the assumed increase in the baseline only reflects those requests that are made directly to the database today. No change is to be expected in requests that already are made through judicial cooperation today (e.g. privacy and proxy services).
        - Service providers: **-50%** in relation to the baseline.
            - Idem public authorities.
            - The % change is in relation with the number of attempts in the baseline.
    - Direct cooperation:
        - Public authorities: 0**%** in relation to the baseline.
            - No change is to be expected as there would be no need to resort to direct requests if access to the database system can be continued.
        - Service providers: **0%** in relation to the baseline.
            - Idem public authorities.
    - Direct access:
        - Public authorities: **0%** in relation to the baseline.

- No impact since this measure does not affect the number of direct access attempts.

The table below summarises the above modifiers for this measure:

| | Judicial cooperation | | Direct cooperation | | Direct access |
|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities |
| Time/attempt (min) | 0% | 0% | 0% | 0% | 0% |
| Attempts | -50% | | 0% | | 0% |

4) Total time.
It was automatically calculated using the above assumptions following the same reasoning as in the baseline.

5) Total continuous costs.
It was automatically calculated using the above assumptions following the same reasoning as in the baseline.

The table below summarises the total continuous costs per year for this measure:

| | Judicial cooperation | | Direct cooperation | | Direct access | Total per year |
|---|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities | |
| Time/attempt (min) | 321 | 146 | 118 | 146 | 64 | |
| Attempts | 30,709 | | 264,534 | | 61,417 | **356,660** |
| Total time (min) | 9,857,447 | 4,483,450 | 31,215,035 | 38,621,993 | 3,942,979 | **88,120,904** |
| | | | | | ***Total continuous costs per year*** | ***€ 44,060,452*** |

Measure 7: legal framework for direct access

1) One-off costs.
   - Public authorities:
     - Transpose EU legislation:
       - 100 working days x 27 Member States: time of 100 working days based on a previous Commission study[188]. Assumes all Member States would take part, except DK.
       - Assumes that the instrument would be a directive. If the instrument were a regulation it would not require transposition.
2) Time per attempt per channel.
   - Judicial cooperation:

[188] Study for an impact assessment on a proposal for a new legal framework on identity theft, 2012, p160.

- Public authorities: **0%** in relation to the baseline.
  - No impact since this measure does not affect judicial cooperation times.
- Service providers: **0%** in relation to the baseline.
  - No impact since this measure does not affect judicial cooperation times.

- Direct cooperation:
  - Public authorities: **0%** in relation to the baseline.
    - No impact since this measure does not affect the direct cooperation times.
  - Service providers: **0%** in relation to the baseline.
    - No impact since this measure does not affect the direct cooperation times.
- Direct access:
  - Public authorities: **+5%** in relation to the baseline.
    - Additional time to ensure compliance with safeguards and statistics.
    - No significant change in time expected as most Member States already have rules in place that would need to be slightly adapted, if at all.

3) Total number of attempts per channel.
   - Judicial cooperation:
     - Public authorities: -3**%** in relation to the baseline.
       - Transfer of requests from judicial cooperation to direct access from Member States that do not have direct access today and need to rely on judicial cooperation (possibly unsuccessfully).
     - Service providers: -3**%** in relation to the baseline.
       - Idem public authorities.
       - The % change is in relation with the number of attempts in the baseline.
   - Direct cooperation:
     - Public authorities: **0%** in relation to the baseline.
       - No impact since this measure does not affect the number of direct cooperation attempts.
     - Service providers: **0%** in relation to the baseline.
       - No impact since this measure does not affect the number of direct cooperation attempts.
   - Direct access:
     - Public authorities: **+15%** in relation to the baseline.
       - Use of direct access subject to conditions and safeguards in cases which today are not clearly addressed by the present-day legal framework.

- Transfer of requests from judicial cooperation to direct access from Member States that do not have direct access today and need to rely on judicial cooperation (possibly unsuccessfully).

The table below summarises the above modifiers for this measure:

| | Judicial cooperation | | Direct cooperation | | Direct access |
|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities |
| Time/attempt (min) | 0% | 0% | 0% | 0% | 5% |
| Attempts | -3% | | 0% | | 15% |

4) Total time.
It was automatically calculated using the above assumptions following the same reasoning as in the baseline.

5) Total continuous costs.
It was automatically calculated using the above assumptions following the same reasoning as in the baseline.

The table below summarises the total continuous costs per year for this measure:

| | Judicial cooperation | | Direct cooperation | | Direct access | Total per year |
|---|---|---|---|---|---|---|
| | Public authorities | Service providers | Public authorities | Service providers | Public authorities | |
| Time/attempt (min) | 321 | 146 | 118 | 146 | 67 | |
| Attempts | 59,575 | | 264,534 | | 70,630 | **394,738** |
| Total time (min) | 19,123,448 | 8,697,892 | 31,215,035 | 38,621,993 | 4,761,147 | **102,419,515** |
| | | | | | ***Total continuous costs per year*** | ***€ 51,209,757*** |

## 3. Limitations

- The estimated cost of each **policy option** was assumed to be the **sum** of the estimated costs of the **policy measures** it is made of. This could lead to an **overestimation** of the costs, since some economies can occur when developing/transposing legislation combining two or more legislative and/or non-legislative measures.
- The estimates in the model consider the averages of **content/non-content** requests and requests **within the EU and with non-EU countries,** so it does not allow for the breakdown of the results based on these variables.

## ANNEX 5: LIST OF RELEVANT LEGISLATION AND POLICIES

The following legislative instruments and policies are relevant for improving cross-border access to electronic evidence:

### 1. EU cooperation mechanisms in criminal matters

Cooperation mechanisms facilitate cross-border investigations and coordination of prosecutions. These include:

- Directive 2014/41/EU regarding the **European Investigation Order** in criminal matters[189] (EIO Directive), in application since May 2017. It is based on mutual recognition of judicial decisions, and updated the legal framework applicable to the gathering and transfer of evidence between Member States. In particular, it replaced the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[190], which sets out the conditions for mutual legal assistance. This Directive allows an authority in one Member State (the "issuing authority") to request that specific criminal investigative measures be carried out by an authority in another Member State (the "executing authority"). The EIO Directive covers any investigative measure except for joint investigation teams (cf. Art. 3). This means all types of evidence are covered, including electronic evidence. While the EIO Directive contains specific provisions on the interception of telecommunications, it does not contain any specific provisions on **access** to electronic evidence, except for a reference to the identification of a person holding an IP address in Art. 10(2)(e), for which double criminality cannot be invoked as ground for refusal.
- Council Decision 2002/187/JHA setting up **Eurojust**[191], which facilitates cross-border judicial cooperation in criminal matters. The **European Judicial Cybercrime Network**, supported by Eurojust and established by Council conclusions on 9 June 2016[192], brings together judicial authorities from the EU Member States with the objective to facilitate and enhance cooperation between the competent judicial authorities dealing with cybercrime, cyber-enabled crime and investigations in cyberspace.

---

189 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, p.1.

190 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

191 Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime.
The Commission adopted in 2013 a proposal for a Regulation to reform Eurojust (Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust), COM/2013/0535 final.

192 Council conclusions of 9 June 2016 on the European Judicial Cybercrime Network, 10025/16.

- Regulation (EU) 2016/794 on **Europol**[193], which sets up the rules for Europol, in particular its objectives, tasks and scrutiny, including monitoring of Europol's processing of personal data.
- Council Framework Decision 2002/465/JHA on **joint investigation teams**[194] sets up rules on the creation of such teams for carrying out criminal investigations.
- An initiative is ongoing to ensure the future financing and governance of the **e-CODEX** system. e-CODEX is an IT system developed by a consortium of Member States for cross border judicial cooperation which allows users, be they judicial authorities, legal practitioners or citizens, to send and receive documents, legal forms, evidence or other information in a secure manner. e-CODEX is the cornerstone of the upcoming EIO platform, which is being developed by the Commission as one of the practical measures under the e-evidence initiative. The eCodex project was not included in the baseline as it is still under development and the degree to which it would be implemented in relation to cross-border access to e-evidence is still unclear. Given the range of possible outcomes of the e-Codex project, it was preferred to evaluate it as part of one of the practical measures rather than as part of the baseline. Since the evaluation of impacts of the policy options is done in relation to the baseline, it was preferred to consider a more stable baseline without e-Codex.
- Finally, the **Commission's Communication on Tackling illegal content online** from 28 September 2017, while calling for a prompt removal of illegal content by online intermediaries, highlighted that removal of such content should not impede the prosecution of or other follow-up to any underlying breach of law. Evidence sharing amongst public authorities and online platforms is an important policy in this regard, and reference is also made to the present initiative to facilitate cross-border access to evidence.[195]

## 2. EU data protection legislation

- The legislation resulting from the data protection reform [196] is of critical importance in the context of cross-border access to electronic evidence:
  - Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[197] (**General Data Protection Regulation, GDPR**).

---

193 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

194 Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams.

195 COM(2017)555.

196 See here for more information.

197 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

- Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data[198] (**Police Directive**).

- The 2009 **ePrivacy Directive**[199] ensures that all communications over public networks maintain respect for fundamental rights, in particular a high level of data protection and of privacy, regardless of the technology used. In January 2017 the Commission adopted a proposal for a Regulation on Privacy and Electronic Communications[200] to replace the 2009 Directive. This proposal is still under negotiation.

The following recent proposals, also under negotiation by the European Parliament and the Council, are also relevant:

- The proposal for a Regulation on a framework for the **free flow of non-personal data** in the European Union[201] aims to facilitate the storage and processing of non-personal data across the Union to contribute to the building of the European data economy and boost the competitiveness of European businesses, while enhancing the availability of modern data storage and processing services to public authorities. Article 5 foresees a general cooperation mechanism for national authorities to obtain access to data stored in another Member State, to be applied only if no specific cooperation mechanism exists under Union law or international agreements to exchange data between competent authorities of different Member States.
- Although not directly dealing with data protection, the proposal for a Directive establishing the **European Electronic Communications Code** (Recast)[202] is

198 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

199 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

200 Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final.

201 Proposal for a Regulation of the European Parliament and the Council on a framework for the free flow of non-personal data in the European Union, COM(2017) 495 final.

202 Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), COM(2016) 590.

important for data protection considerations and cross-border access to data, as it modernises its scope of application (i.e. the definition of electronic communications service) and aims to contribute to ubiquitous connectivity in the internal market, which would likely increase significantly the volume of data generated.

### 3. Others

- The **E-commerce Directive 2000/31** [203] establishes the free provision of information society services inside the EU. These services providers (which are also partially within the scope of the present initiative) should be subject only to the rules applicable in their country of establishment and Member States cannot restrict the provision of such services in the coordinated field. However, they can apply their national rules on criminal law and criminal proceedings with a view to taking all investigative and other measures necessary for the detection and prosecution of criminal offences, without there being a need to respect the notification procedure under this Directive (Recital 26). Private law disputes are not covered by this exception.
- The **proposal for a Directive to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market** [204] is also important for data protection considerations and cross-border access to data. This proposal clarifies that national competition authorities should have access to data accessible to a company in the EU, even if that data is stored in the cloud or held by a parent company in another Member State or outside of the EU.
- Two other ongoing initiatives concern the **taking of evidence** and the **serving of documents** in civil judicial procedures. Both initiatives aim among others to modernise existing instruments with a view to digitalisation. One of the aims of the initiative to revise the existing Regulation 1206/2001 on taking of evidence in civil and commercial matters [205] is to adapt the system to the technical developments provided by the digitalisation (thereby facilitating the switch from paper-based channels to electronic ones), to ensure mutual recognition of domestic systems of electronic service of documents and electronic evidence.

### 4. International law (involving non-EU countries):

---

[203] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[204] Proposal for a Directive of the European Parliament and of the Council to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, COM(2017) 142 final.

[205] Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters, OJ L 174, 27.06.2001, pp. 1-24.

- **Multilateral agreements:**
  - Council of Europe **Convention on Cybercrime** (Budapest Convention). [206] This 2001 instrument provides, among others, a framework for mutual legal assistance and a definition of electronic evidence. The Parties have recently started negotiating an additional protocol to the Convention dealing with cross-border access to e-evidence.
- **Bilateral agreements**:
  - Between the EU and non-EU countries, such as the 2000 Agreement on **Mutual Legal Assistance between the EU and the US**[207]. The EU-US **Umbrella Agreement**[208] complements existing EU-US and Member State –US agreements by a comprehensive high-level data protection framework for EU-US law enforcement cooperation. The **EU-US Privacy Shield**[209], a data-sharing agreement which ensures the flow of personal information for commercial purposes across the Atlantic, is also relevant.
  - Between **EU Member States and non-EU countries on mutual legal assistance**. A large number of them exist[210].

    It has been reported that the **UK and the US** are currently negotiating a bilateral agreement that would permit UK-based law enforcement to request stored communications and live intercepts directly from US-based providers, including content data, as an alternative to MLAT (on a reciprocal basis).[211]

## 5. National law

- **Of Member States**, since some of them have adopted national provisions to facilitate cross-border access to electronic evidence, for example through **direct access** (see section 2).
- **Of non-EU countries**: since many of the service providers whose cooperation is required to obtain certain types of electronic evidence are headquartered in the

---

206 Council of Europe Convention on Cybercrime (CETS No 185).

207 Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America.

208 More information on the EU-US Umbrella Agreement is available here.

209 More information on the EU-US Privacy Shield is available here.

210 See for instance the Treaty between the Kingdom of the Netherlands and the United States of America on mutual assistance in criminal matters of June 1983.

211 Daskal, Jennifer, A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right, February 2016;
Lin, Tiffany and Fidler, Mailyn, Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement, Berkman Klein Center Research Publication No. 2017-7, Harvard University, September 2017.

US or other non-EU countries, the internal legal framework of those non-EU countries is also relevant in this context. In particular, the national **US law** of relevance includes:

- the Electronic Communications Privacy Act of 1986[212] ;
- a proposal put forward by the US Department of Justice in 2016 and 2017[213] to improve the current access to e-evidence[214] (see Annex 10);
- the International Communications Privacy Act[215], a bipartisan proposal that aims to clarify US law enforcement's ability to obtain e-evidence while respecting privacy laws of other countries.

## 6. EU policy

In addition to the above legislative instruments, three important EU policies are key to understand the context of improving cross-border access to e-evidence:

- the **European Agenda on Security**[216], which sets out the principles for EU action to respond effectively to security threats and the main steps planned by the European Commission to implement these, and identifies the 3 priorities for immediate action, by both national governments and the EU institutions, which share responsibility for EU security: 1) preventing terrorism and countering radicalisation; 2) fighting organised crime; 3) fighting cybercrime.
- the **EU Cybersecurity Strategy**[217], which aims at creating the world's most secure online environment in the EU, by providing for partnerships with the private sector and non-governmental organisations or interest groups, and concrete action to protect and promote citizens' rights. This strategy was reinforced with the adoption of the Cybersecurity Package in September 2017[218], which included a proposal for an EU Cybersecurity Agency, proposals to step up EU's cybersecurity capacity and proposals to create an effective criminal law

---

212 Electronic Communications Privacy Act of 1986; see Annex 6 for more information.

213 U.S. Department of Justice, Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism, July 15, 2016.

214 On 23 March 2018 the US Congress adopted the Clarifying Lawful Overseas Use of Data (CLOUD) Act, right before the adoption of the EU legislative proposals that this impact assessment accompanies. The CLOUD Act is available here.

215 S.1671 - International Communications Privacy Act.

216 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security, COM(2015) 185 final.

217 Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace (JOIN(2013) 1 final of 7.2.2013).

218 More information is available here.

response. It also highlighted the availability and accuracy of WHOIS data as a key priority[219].

- the **Digital Single Market Strategy**[220], which sets out 16 targeted actions based on 3 pillars: 1) Better access for consumers to digital goods and services across Europe, 2) Creating the right conditions and a level playing field for digital networks and innovative services to flourish and 3) Maximising the growth potential of the digital economy.

On **encryption**, the Commission proposed in October 2017 a set of measures to support law enforcement in addressing the challenges posed by the use of encryption by criminals, following consultations on technical and legal aspects with relevant stakeholders[221]. These included experts from Europol, Eurojust, the European Judicial Cybercrime Network (EJCN), the European Union Agency for Network and Information Security (ENISA), the European Union Agency for Fundamental Rights (FRA) and Member States' law enforcement agencies, industry and civil society organisations.

Two sets of measures were proposed to support law enforcement in addressing the encryption challenges, without **prohibiting, limiting or weakening encryption** (e.g. no "backdoors"):

- Legal framework for cross-border access to electronic evidence (i.e. the initiative addressed in this impact assessment), including a set of practical measures to facilitate access.
- Technical measures, including supporting Europol to develop its decryption capability, setting up a network of points of expertise in Member States to exchange decryption techniques, facilitating dialogue with service providers and providing training programs for public authorities.

In the absence of EU action to improve cross-border access to e-evidence (i.e. legal measures described above), an important part of the measures proposed to help law enforcement address encryption challenges would not materialise.

---

[219] The importance of WHOIS data was also echoed in the Council Conclusions of 20 November 2017 on the Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 14435/17. Specifically, the Council "stresses the importance of ensuring a coordinated EU position to efficiently shape the European and global internet governance decisions within the multi-stakeholder community, such as ensuring swiftly accessible and accurate WHOIS databases of IP-addresses and domain names, so that law enforcement capabilities and public interests are safeguarded."

[220] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe - COM(2015) 192 final.

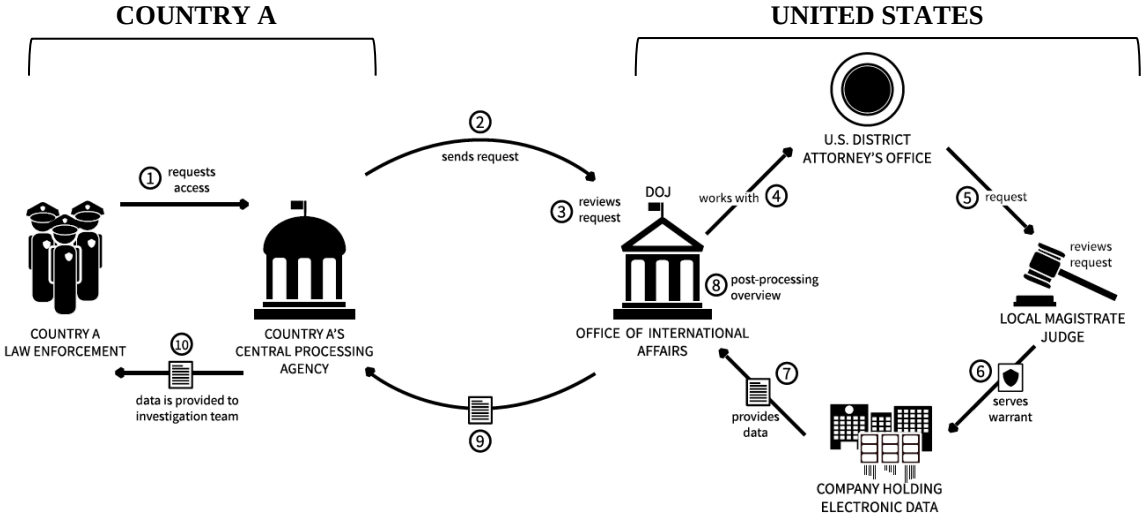
[221] Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union, COM(2017) 608 final, 18 October 2017.

## ANNEX 6: ADDITIONAL INFORMATION ON THE PROBLEM DRIVERS

1. It takes too long to access e-evidence across borders under existing judicial cooperation procedures, rendering investigations and prosecutions less effective.

The following figure describes a typical MLAT process between a given country A (e.g. a Member State) and the US for requests of access to e-evidence:

*Figure 1: MLAT process between a Member State (country A) and the US*




Source: Harvard University[222]

The process is the following[223]:

1. Law enforcement in country A, typically under judicial supervision, desiring access to data held by a US service provider, obtains internal and sometimes also regional approval to file a request with their country's designated central authority, which reviews the request.
2. Once approved, public authorities in country A send the request to the US Department of Justice's (DOJ) Office of International Affairs (OIA).
3. The OIA works with the public authorities of country A to revise the request's format and content to meet US standards.
4. Once the OIA is satisfied, OIA works with a US District Attorney's Office to send the request to a local US magistrate judge for review.
5. The court must find that the request is in keeping with all relevant US law, notably including the Fourth Amendment's **probable cause** standard where content data is concerned, rules of privilege, and the Fifth Amendment's right to avoid self-incrimination. If any of these are not met, the OIA and the requesting country's agency continue to work together until the court is satisfied.

222 Lin, Tiffany and Fidler, Mailyn, Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement, Berkman Klein Center Research Publication No. 2017-7, Harvard University, September 2017.

223 *Ibid.*

6. Once approved by the court and thus translated into a national order, the **request is served** on the service provider.
7. Once the service provider receives the request, it locates and submits the relevant evidence to the OIA.
8. The OIA **reviews the evidence** to ensure it meets data minimisation and human rights standards.
9. Finally, the evidence is sent back to the requesting country's central processing agency.
10. The central processing agency provides the evidence to the original investigating team.

There were extensive consultations in the EU and the US to determine the reasons that explain the long duration of the MLAT process. These consultations included a fact-finding mission to the US to discuss in person with OIA representatives in the Department of Justice, as well as with Member States liaison magistrates that facilitate the communication between public authorities in the Member States and the OIA. The analysis below also includes the findings of the five year review of the EU-US MLA agreement carried out in 2016, as well as those of previous assessments[224].

The stakeholders identified the **high volume of requests** to access e-evidence as the main factor that has put the MLAT system under enormous strain, and has shown its weakness to deal effectively with the current needs. Although exact data of incoming MLAT requests is not available, the OIA indicated that it receives around 30 new requests per week, a majority of which comes from Europe. In their 2015 fiscal year budget request, the Department of Justice stated that "request for assistance from foreign authorities had increased nearly **60 percent**, and the number of requests for computer records has increased **ten-fold**" over the past decade, slowing processing times[225]. In 2016 OIA received around 1600 requests, a number that had been already overtaken by October 2017. There is a backlog of around 2000 requests globally. In an effort to improve the situation, the US Department of Justice created a dedicated team for electronic evidence and obtained a change in legislation allowing them to make the relevant pleas before the local District of Columbia courts. Nonetheless, resources continue to be overwhelmed by the swift growth in requests and response times have not significantly decreased.

In addition to the high volume of requests, stakeholders identified the following three main factors that determine the response times:

[224] See in particular:
- Council of Europe Budapest Convention on Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, December 2014;
- Discussion paper on tackling cybercrime, Informal Meeting of the Justice and Home Affairs Ministers, Amsterdam 25-26 January 2016.

[225] U.S. Department of Justice, FY 2015 Budget Facts Sheet, 2015.

1) **Quality of the request**.

The quality of the request can make the response time vary significantly. The complexity of the MLAT procedures requires specific expertise to prepare the requests, in particular with regard to the US' legal system. The more the request follows the required standards the fewer the iterations required between the OIA and the public authorities of the Member State, and the faster the process can be.

Some of the most common issues encountered in MLAT applications are:

- Unclear **probable cause** in requests for content, e.g. the connection between the criminal activity and the account is unclear. In some cases, it might not be possible to gather all the data required to prove probable cause under US standards, in particular in the initial stages of case. In other cases, there can be a lack of understanding in Member States of the US legal system, due to the different legal traditions, including with regard to fundamental rights, and in particular freedom of speech. Also, these different legal systems use different legal terms that might be challenging to translate (e.g. the translation into English may be more representative of the UK legal system than the US one).
- Missing information, in particular the **timeframe** relevant to the e-evidence sought. For example, the request does not specify the timeframe in which a potential criminal activity could have occurred in a suspect's Facebook account.
- Since summer 2016, as a consequence of the Microsoft Ireland Court of Appeal ruling,[226] the DOJ has been asking foreign authorities filing MLA requests for e-evidence to first **verify with service providers that the data is stored in the US**. This further increases the time of the MLAT procedure (e.g. Microsoft recently announced that they needed 6 weeks to identify the location of data). If the data is stored in a country other than the US, the DOJ generally finds itself unable to answer the MLA request.
- Paper submission: some countries submit the requests **on paper**, when there is no need for that on the US side. The US authorities are in the process of making available an email mailbox to receive electronically the incoming requests and could provide formal paper documents if needed, after the request has been handled electronically.

The request is more likely to suffer from the above and other quality issues in the absence of a **central authority** in the Member State (not all of them have it) or in the absence of effective centralised procedures that serve as quality control (MLAT treaties typically do not require the existence or use of a central authority).

[226] See Box 1 in Annex 9 on the Microsoft case.

2) **Type of request**.

The requests for **content** take much longer than the requests for non-content, as the former require higher standards such as proving probable cause[227] (see step 5 above) and undergo more complex procedures such as:

- **search warrant** (step 6 above), in which the service provider is requested to make available all the information in a given account in the timeframe indicated[228];
- **filtering** (step 8 above), or data minimisation, in which an FBI agent reviews all the content provided to determine what is relevant to the offence and can be forwarded to the requesting country. This step can be particularly time consuming as not only the amount of content to review can be significant but also because translations may be required. The requesting country is not informed of what has been filtered out.

*Box 1: ECPA, the US law that shapes the current procedure for accessing e-evidence held by US service providers*[229]

Countries must follow the MLAT process to access data held in the US because US law (**ECPA** [230]) currently restricts the possibilities of US companies to disclose information to government entities. These restrictions have been interpreted to cover any government entity, including foreign governments.

**Why content requests take the longest:**

ECPA (specifically, Title II of ECPA, also called the **Stored Communications Act**) contains blanket restrictions that prohibit US companies from sharing the content of stored electronic communications with government entities, other than pursuant to a US warrant or consent of the user[231].

**Why non-content requests are faster:**

Companies are allowed to disclose voluntarily non-content data (subscriber information and metadata) to foreign governments directly upon request. While US government agencies must obtain a US court order, this is not required of foreign authorities[232]. However, the laws of most EU Member States also require a court order to request non-content data, including for such direct cooperation requests. Where companies agree to comply with the non-

227 The standards to accept content requests are the same for domestic as for international requests.

228 The authorities of the requesting Member State do not see the U.S. search warrant.

229 Lin, Tiffany and Fidler, Mailyn, Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement, Berkman Klein Center Research Publication No. 2017-7, Harvard University, September 2017.

230 Electronic Communications Privacy Act of 1986, An Act to amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes.

231 *Ibid*, 18 U.S.C. §§ 2701 et seq.

232 18 U.S.C. §§ 2702(c)(6), 2711(4). See also David Kris, Preliminary Thoughts on Cross-Border Data Access, Lawfare, September 28, 2015.

binding requests from foreign authorities, the procedure is faster because the separate full review by US authorities is skipped.

**Why emergency requests (even for content) are the fastest**:
Companies are able to disclose content information voluntarily in the event of an emergency[233]. For example, in 2015, Microsoft responded to requests for contents of email 45 minutes after the Charlie Hebdo attacks. It did so similarly after the November 2015 Paris attacks[234].

ECPA was introduced in 1986 and there have been repeated calls for its reform, to adapt it to the technological realities of today.

3) **Service providers' internal procedures**.
The time that a service provider takes to process a request varies depending on its internal procedures. Member State authorities pointed out the **lack of transparency** of these procedures[235]:
   - The service provider does not indicate the time that it will take to respond.
   - The criteria that the service provider uses to process the request are unclear.
   - There is often no feedback given to the Member State on the reasons for non-compliance.

2. Inefficiencies in public-private cooperation between service providers and public authorities hamper effective investigations and prosecutions.

Stakeholders expressed general and practical concerns:
- General:
   1) transparency of the process;
   2) reliability of stakeholders;
   3) accountability of stakeholders;
   4) admissibility of evidence;
   5) unequal treatment of Member States;
   6) reimbursement of service providers' costs;
- Practical:
   7) for authorities, how to identify and contact the relevant service provider;
   8) for service providers, how to assess the authenticity and legitimacy of a request.

1) **Transparency** of the process.
A lack of transparency is cited as an issue from several perspectives:

233 18 U.S.C. § 2702(b)(8).
234 Dina Bass, Microsoft Got 14 Data Requests on Paris Suspects, Smith Says," Bloomberg, March 1, 2016.
235 In general, public authorities in the requesting Member State are often unaware of the state of play of a request, after they send it through the MLAT procedure.

- *Service providers* have data protection obligations and wish to make it clear to the public that they take these obligations seriously, disclosing data only on the basis of a valid and legal request and notifying users where possible. However, sharing information about requests received may compromise an investigation. Service providers have therefore started to publish regular **transparency reports** based on aggregated data to prevent being seen as insufficiently transparent about protecting and disclosing customer information.
- One of the major complaints from *law enforcement authorities* concerns the lack of transparency on the providers' side in relation to why a specific request is granted or refused and in which time frame. Investigating authorities often do not understand which arguments and procedures determine the final decision of the requested service provider.
- Stakeholders highlighted the need to ensure **the protection of rights to privacy** and provide measures to that extent, including user notification. The majority of providers underlined the importance of user notification, which should only exceptionally be deferred or prohibited.[236] Any such exceptions should be specific and not provide for indefinite blanket coverage.
- **User notification**, as a tool for transparency, creates its own challenges in cross-border situations for all parties involved, as national laws and company policies provide for different modalities and exceptions for user notification. In some Member States, it is obligatory for the investigating authority to provide notice to the user of an investigative act as long as it does not jeopardise the investigations; in others, the notification is prohibited. The rules on when notice has to take place also vary widely. Service providers indicated that it is often unclear to them from law enforcement requests and applicable rules whether they are allowed to notify a customer, and if not, whether a law enforcement authority will do it and under which conditions. This can lead to situations where Member States' authorities request data from a US provider without realising that the provider will notify the user concerned unless a specific request to refrain from immediate notice is made and granted; this in turn may compromise an investigation under way.
- Transparent information and fair processing are core principles of EU data protection rules; access, rectification and erasure rights are also guaranteed. However, restrictions might be imposed by way of legislative measures to safeguard, inter alia, public security or the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties[237].

---

236 Under U.S. legislation (ECPA), authorities are obliged to notify, and service providers are allowed to notify, unless a court order imposes a temporary block on notification.

237 See Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); and Article 13(3) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

2) **Reliability** of stakeholders.

The process, regulated only through individual company policy on the provider side, is **not predictable** and thus not reliable for both service providers and law enforcement authorities. Data availability and service providers' requirements and conditions for providing that data vary widely, as does the quality of law enforcement requests.

- *Service providers* complain about the wide variety of request formats and about requests sent in a way that prevents authentication, e.g. if no secure channel of communication is used or the request is sent to a general info or press mailbox. Where forms are made available, they may be poorly filled out, sometimes due to language issues. Issuing authorities sometimes omit contact details, making follow-up questions difficult.
- For *law enforcement authorities*, it can be unpredictable whether a request will be answered at all. As the cooperation takes place on a voluntary basis, providers are under no obligation to state reasons for refusal of disclosure or even to respond at all. Major service providers' approaches also differ with regard to the law enforcement agencies they will respond to, the supporting documentation they require, and the link to the investigating country that they demand. For example, some service providers do not request details of the case under investigation, while others do; also while one provider may require that an underlying IP address resolve to the investigating country, another will provide data as long as the IP address does not resolve to the US. In addition, there are no binding deadlines for responses.
- Besides the larger service providers which have often already established a range of different channels and policies to deal with requests, there is also a growing number of smaller service providers and a plethora of apps that can become relevant in criminal investigations. In these situations, experts highlighted that cooperation was often more challenging because both sides were unfamiliar with each other, there was a lack of specific rules and policies, and a lack of familiarity with the framework.
- Even if law enforcement authorities are aware of certain procedures required by a company at a certain point of time, providers may change their policies at any time without notice.

3) **Accountability** of stakeholders.

The problems of lacking accountability go hand in hand with those of transparency and reliability.

- *Service providers* frequently have no insight into which crimes are being investigated as this may be confidential information. This makes it difficult for the providers to be accountable to their users. As data is provided without a legal obligation under US law, service providers are also not accountable to law enforcement authorities for submitting no, incomplete or even false information. Requests are not enforceable under US law (this would require going through mutual legal assistance instead).
- In relation to privacy and data protection, stakeholders from the private sector also highlighted the specific expectations of **corporate customers** that a provider of

corporate systems and services should in principle not be asked to provide information pertaining to their corporate client. Rather, it was pointed out, authorities should consider requesting the information from the corporate client itself.

- *Law enforcement authorities* are held accountable through various processes including the need for prior authorisation by a judge and the possibility to refute admissibility of evidence gathered in violation of procedural rules in a subsequent court proceeding. However, these processes are usually not designed to take account of this direct cooperation across borders and therefore are deemed unsatisfactory by some.

4) **Admissibility** of evidence.
Given that direct requests from law enforcement authorities in an EU Member State to service providers established elsewhere are not explicitly foreseen under most national laws of criminal procedure, there can be problems with the admissibility of evidence gathered through direct cooperation in a subsequent criminal trial, both for requests that undergo individualised review and for database searches. This is also highlighted in the GENVAL Final Report, which refers to the specific challenges arising from the nature of e-evidence and the ease with which it can be manipulated or falsified[238].

5) **Unequal treatment** of Member States.
*Law enforcement authorities* from different Member States indicate that providers respond differently depending on where requests come from. This is confirmed by an analysis of transparency reports of some of the major service providers: the average percentage of disclosure of data following all requests sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2014 varied among EU Member States from 31 % (Poland) up to 78 % (the Netherlands) [239].

The following tables illustrate the problem, using data from 2014 transparency reports of the respective companies[240]:

*Table 1: range of rate of disclosure by Member State*

| Service provider | Range of rate of disclosure |
|---|---|
| Google / Youtube | 0 % (Hungary) - 83 % (Finland) |
| Facebook | 15 % (Austria) - 80 % (Croatia) |
| Apple | 29 % (France) - 90 % (Austria) |

238 GENVAL Final Report on the Seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime" ("GENVAL Report"), ST 9986/17, p. 50.

239 Council of Europe Budapest Convention on Cybercrime Convention Committee (T-CY), Criminal justice access to data in the cloud: Cooperation with "foreign" service providers, T-CY (2016)2, provisional document of 3 May 2016.

240 Transparency reports of Apple, Facebook, Google and Microsoft.

*Table 2: range of rate of disclosure by service provider*

| Member State | Range of rate of disclosure |
|---|---|
| Austria | 27 % (Google / Youtube) - 90 % (Apple) |
| Germany | 38 % (Google / Youtube) – 79 % (Microsoft/Skype) |
| Hungary | 34 % (Facebook) - 83 % (Microsoft / Skype) |
| Slovakia | 8 % (Google / Youtube) – 81 % (Microsoft/Skype) |

In addition, there are a number of providers which do not reply to any requests at all.

6) **Reimbursement** of service providers' costs.
While service providers usually receive some form of **cost reimbursement** in relation to requests made in the domestic setting, notably domestic providers of telecommunications services, this is different when considering cross-border requests.
   - Several US-based service providers indicated that they currently respond to law enforcement requests without asking for a reimbursement of related costs.
   - Linked to this, some stakeholders have stressed that smaller companies may struggle to meet requirements that larger companies might be able to meet comparatively easily because of their scale.
   - In relation to possible new obligations, it was pointed out that service providers might incur unforeseen expenses.
   - Some stakeholders suggested that a requirement for a reimbursement of costs could also be seen as a safeguard to ensure that the authorities' requests are limited to the absolute minimum.

7) How to **identify and contact** the relevant service provider.
   - *Law enforcement authorities* report problems in identifying which service provider can provide data on, e.g., an email account encountered during the investigation. Furthermore, while most service providers offer a special **point of contact** for an official request, these contact points may be at national level, set up for regions (like Europe), or directly at the seat of the company which may be anywhere in the world.
   - Even if the contact point has been clarified for a specific case, establishing actual contact can still be difficult: there is no common line among providers regarding the use of platforms, forms, required content of a request, language or communication channels. Law enforcement authorities have to tailor their approach to each individual company.

8) How to assess the **authenticity and legitimacy** of a request.
   - Most *service providers* assess whether the request complies with the domestic legal framework of the requesting authority. This extends to checking whether the

requesting authority would have the power to request a certain type of data from a service provider at the domestic level, as a direct request to a foreign service provider, while permissible, is usually not explicitly provided for in national legislation. Taking this assessment seriously creates significant legal expenses for providers, especially since national provisions differ widely even among Member States.

- Furthermore, in order to avoid civil and/or criminal liability for sharing data with unauthorised parties, service providers have to ensure authenticity of the request. This can be difficult.
- Member States' *law enforcement and judicial authorities* frequently view the assessment of compliance with national law as inappropriate. In their view, it should not be up to a private company to privately challenge a judicial assessment on whether conditions under national law for the disclosure of data are met. However, as there are no enforcement mechanisms attached to this form of cooperation, the service provider's assessment determines compliance.

3. Shortcomings in defining jurisdiction can hinder effective cross-border investigations and prosecutions.

   See section 2.2.3.

## ANNEX 7: ADDITIONAL INFORMATION ON THE POLICY MEASURES

### Non-legislative action

Measure 1: practical measures to enhance judicial cooperation

*a) Judicial cooperation with the US (MLA)*

The expert consultation process identified the following practical measures to enhance judicial cooperation between **public authorities in the EU and the US**, on the basis of the existing mutual legal assistance procedures:

1) **Organise regular technical dialogues with the US Department of Justice** to continue to improve the process, speed and success rate of MLA requests for e-evidence, in particular in relation to content data. In order to ensure a common approach and to avoid conflicts of law, both the EU and the US could benefit from a closer collaboration, including through visits, to work not only on practical aspects but also to discuss legislative developments on both sides of the Atlantic. Applicable law in the US is currently subject to review, and conflicting legislative approaches between the EU and the US should be avoided. At the December 2016 EU-US Justice and Home Affairs Ministerial meeting, it was already agreed to step up the collaboration on cybercrime, including on cross-border access to electronic evidence[241]. Regular videoconferences and phone calls have taken place since (see Annex 2). Collaboration could be continued and expanded.

2) **Facilitate regular contacts between the EU Delegation to the US, the Commission and liaison magistrates** of Member States in the US to discuss issues affecting the MLA process. EU Member States liaison magistrates have significant operational experience in the MLA process and play a key role in facilitating the communication between EU and US judicial authorities. Their experience can be a source of information on the issues faced and on possible practical/legislative solutions. As part of the expert consultation process, the Commission and the EU Delegation to the US facilitated a number of meetings, which provided for an opportunity to share experiences and to learn about practical problems liaison magistrates of Member States are facing in their day-to-day work on cross-border access to electronic evidence, both on the basis of direct cooperation and on the basis of mutual legal assistance procedures. The Commission and the EU Delegation could continue to facilitate such regular contacts to ensure that both policy development and practical cooperation benefit from the expert input of the liaison magistrates.

3) **Provide opportunities for the exchange of best practice and further training** for EU practitioners on applicable rules in the US relate to the MLA procedure. The Commission

[241] Joint EU-US statement following the EU-US Justice and Home Affairs Ministerial meeting of 5 December 2016, Doc. 722/16.

has made available **EUR 500 000** under the Partnership Instrument[242] to fund the creation of training materials and the organisation of courses, meetings and conferences. Some examples of exchanges of best practice and further trainings could include:

- Training on US legal concepts, including the criterion of **probable cause** relevant for access to content, how to draft an order, how to draft complementary records to e.g. prove probable cause or MLA checklists.
- Sharing/centralisation of training materials at EU level in a single website. Now each liaison magistrate prepares MLA guidelines on applicable rules and procedures for his/her own country's judges243. Centralising the guidelines and other training materials in a single website could help facilitate the exchange of best practices and possibly the production of common best practices at EU level, which would also benefit Member States that do not have a liaison magistrate posted to the US.
- The exchange of best practices could also address the workflow and organisation at the national level, in particular with regard to the use of a centralised authority to ensure the quality of the outgoing requests and facilitate communication. Some liaison magistrates also indicated the translation services as another possible area for improvement at national level.
- The trainings could be filmed, subtitled and made available to judicial authorities throughout the EU, possibly through the centralised website described above.

*b) Judicial cooperation within the EU (EIO)*

This measure addresses problem driver 1 on judicial cooperation channels by facilitating the implementation of existing EU law, specifically the Directive 2014/41/EU on the **European Investigation Order** in criminal matters[244] (EIO Directive). This directive, in application since May 2017 and based on mutual recognition of judicial decisions, updated the legal framework applicable to the gathering and transfer of evidence between Member States[245].

The EIO Directive aims to make cross-border investigations faster and more efficient by setting out mandatory deadlines and limiting grounds for refusal. This will to some extent improve the expediency of proceedings, which is the major issue outlined by Member States

---

242 The Commission launched a call for proposals with a budget of EUR 1million total for improving cooperation both between judicial authorities of EU Member States and the US and between EU authorities and US-based service providers on 4 May 2017 under the Partnership Instrument Annual Action Programme 2016 Phase II - International Digital Cooperation - Component D – Cross Border Access to Electronic Evidence (EuropeAid/155907/DH/ACT/Multi). More information is available here.

243 See for example, the guidelines produced by the UK liaison magistrate to the US, Dan Suter, Guide to Obtaining Communication Service Provider Evidence from the United States, 2015.

244 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, p.1.

245 Notably the Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and its protocol, the Council of Europe European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and its two additional protocols, bilateral agreements and provisions of the Schengen Agreement.

concerning the cross-border access to e-evidence within the EU through judicial cooperation channels.

Ireland and Denmark do not participate in it and will continue to rely on MLA channels for their cooperation with other countries, including other Member States.

To facilitate the implementation of the EIO Directive, three expert meetings have been organised in 2016-2017. Further meetings are expected to be organised in 2018-2019 with a view to preparing a report on the application of the EIO Directive[246].

To this date the EIO Directive has not yet been implemented by all participating Member States. The Commission will continue monitoring the implementation process and, whenever necessary, take legal action against Member States for failing to comply with their obligations under EU law.

In addition to supporting Member States through expert meetings and the usual monitoring work of the Commission, this measure also proposes to facilitate the implementation of the EIO Directive through a set of non-legislative/practical measures that could further improve the speed of judicial cooperation requests to access e-evidence within the EU.

These practical measures are:

1) An **electronic user-friendly version** of the forms set out in these annexes of the EIO Directive:
    - annex A, on requesting e-evidence,
    - annex B, on confirmation of receipt of the EIO and
    - annex C, on notification of the interception of telecommunication without technical assistance.

    The electronic format would facilitate completion and translation of the forms, by, e.g., including pre-defined scroll-down menus offering a choice among options rather than free text entry, creating a set of predefined and pre-translated sentences/paragraphs where free entry is needed. The forms themselves would not be modified, as they are part of the legislative act.

    The electronic version of the forms would include guidance that allows practitioners to fill them in without having followed dedicated training.

    A dedicated expert group of representatives of Eurojust, the European Judicial Network (EJN) and the European Judicial Cybercrime Network have already prepared a pilot version which is ready for consultation with Member States.
    The electronic would be made available on the EJN website.

2) A **secure online platform** for electronic exchanges of EIO/MLA requests and replies between EU competent authorities (including on e-evidence).

[246] This report is required by Article 37 of the EIO Directive.

A secure platform could allow for swift and secure exchanges of requests between competent authorities of different Member States. The Commission could prepare and provide a ready-made portal (a reference portal) that Member States could install and use as their national portal.

The platform would also incorporate the electronic version of the EIO forms described above.

The platform would include comprehensive security requirements. Throughout the meetings, a majority of Member States expressed the choice to use **e-CODEX** as the tool for the secure transmission of the data.

*Box 1: what is e-CODEX[247] and how it could be used in the secure online platform?*

"e-CODEX" is an IT system for cross border judicial cooperation which allows users, be they judicial authorities, legal practitioners or citizens, to send and receive documents, legal forms, evidence or other information in a secure manner. It operates as a decentralised network of access points, interlinking national and European IT systems to one another.

Various Member States are already using e-CODEX to support cross border legal procedures both in civil and criminal matters, e.g. for European Payment Orders and small claims and for mutual recognition of financial penalties and custodial sentences.

For example, during an ongoing investigation into a network of drug-sellers, the prosecution service of Cologne discovers that a huge cannabis plantation is being maintained in a storehouse close to the Belgian- Dutch border. The Public Prosecutors Office in Cologne sends a request for search and freeze to the competent judicial authorities in Belgium and the Netherlands using the e-CODEX infrastructure. Within 3 days the prosecutor is informed about the eligibility of the request for legal assistance.

The communication of the requests and the responses in the secure online platform could take place through e-CODEX, with the relevant authorities accessing it through national portals linked to this. These could be supplemented by databases at national level to provide access to very large files, with only a link being sent through e-CODEX.

The Commission has launched an assessment of the impact of various options for maintaining e-CODEX in the long term, which includes

[247] More information about e-CODEX is available in its website.

examining the need for a legal basis[248].

As the establishment of the system requires parallel work by Member States and the Commission, a dedicated project team including representatives of all Member States would be needed. According to the present timeline the system could be operational by the end of 2019.

Although this platform is currently considered to cover the exchanges among EU competent authorities, in the long term it could be extended to facilitate direct cooperation between public authorities and service providers, as well as cooperation with public authorities of non-EU countries.

Measure 2: practical measures to enhance direct cooperation

This measure would address problem driver 2 by making procedures for public-private cooperation more efficient.

The expert consultation process identified and broadly supported the following practical measures to enhance cooperation between public authorities in the EU and service providers, aiming to tackle in particular the issues identified in problem driver 2 (section 2.2.2.):

1) Creation of **single points of contact (SPOC)**, both on the public authorities' side and on the service providers' side:
    - On the **public authorities' side** in the Member States, it could significantly improve the direct cooperation between those authorities and service providers by e.g. ensuring the quality of outgoing requests and build relationships of confidence with providers, as they know their counterpart:
        - A number of Member States (FR, UK, SE, BE, FI, LT) have already created a national central coordinating body for the direct cooperation between law enforcement authorities and service providers. The establishment of SPOCs has resulted in a significant improvement in the efficiency of this channel, both on the side of the authorities in the Member State, and on the side of the service provider.
        - Although no country has collected quantitative data on how the SPOC system has improved its investigations, in general Member States with a SPOC system reported that it served as a filter for overly broad requests or ones that are unlikely to be answered based on a service provider's individual policies; they saw an increase in quality and hence in response rates and a reduction in response times for MLA and direct cooperation;

[248] Inception Impact Assessment – Cross-border e-Justice in Europe (e-CODEX), European Commission, 17 July 2017.

and SPOC systems in general, even with their different current implementations, are uniformly perceived very positively by service providers who say that it improves the quality of requests and helps authenticate requests, as well as allowing them to build a relationship of trust leading to swifter checks and more efficient cooperation.

- The specific feedback from experts from relevant Member States that have put in place SPOC systems depended on the type of system implemented, as there are many different variants in place. For example, the UK SPOC also manages requests to national telecommunication services while the BE SPOC is only in charge of requests to foreign jurisdictions.
- While some SPOCs serve as a channel, others serve as a source of expertise only, e.g. in FR. These SPOCs provide expertise (a sort of central "help desk") on the different policies of service providers. The centralisation of expertise can improve the quality of outgoing requests; some but not all SPOCs also validate each request before it is transferred.
- The SPOCs can also help establish relationships with service providers, which could facilitate the authentication of requests and, in general, reaching cooperation agreements.
- Although not all Member States would have to choose the exact same implementation of SPOCs in their system, e.g. at central or decentralised level, the Commission could consider giving **recommendations** to facilitate their implementation and the development of best practices.

*Box 1: UK SPOC System*

**UK System for Single Points of Contact**

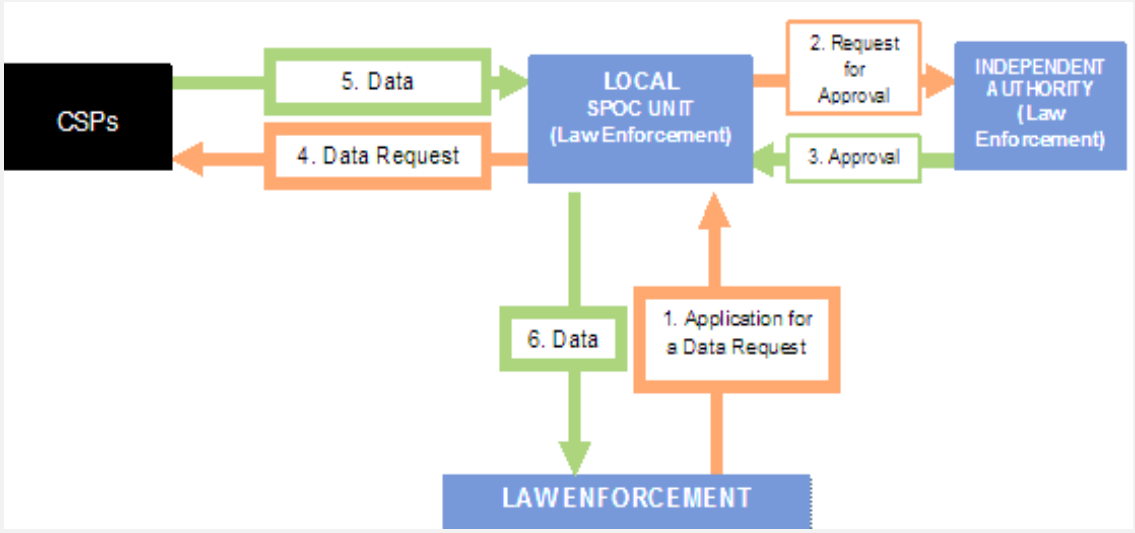
In the UK, authorities are required to make requests for communications data via a Single Point of Contact (SPOC). The code of practice[249] explains that a SPOC: 'promotes efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. This encourages the public authority to regulate itself. The SPOC provides objective judgement and advice to both the applicant and the designated person.'

A SPOC is not responsible for authorising an application; that is done by a designated senior officer in the requesting authority who is independent of the investigation. However, the SPOC will advise the applicant on the application before it is sent to be authorised to ensure it is of a sufficiently high standard. In practice, many more applications are rejected or sent back for reworking by a SPOC, which provides careful scrutiny, than by the authorising officer. Once an application has been authorised, the SPOC acquires the data from the service

[249] A statutory code of practice under the Regulation of Investigatory Powers Act 2000 (RIPA).

provider ("CSP" in the diagram below).

Each member of the SPOC receives a **unique identifier**, which must be provided when making requests. This reassures the service provider that the request is legitimate and that a customer's data is only disclosed to a person who is permitted to acquire it.




- On the **service provider's side,** the creation of a single point of entry could also improve the direct cooperation between those authorities and service providers, by, e.g., helping to clarify the provider's policies:
    - A number of providers, including Apple, Facebook, Google, Microsoft and Twitter, have already taken initiatives ranging from standard forms and dedicated mailboxes that are secured and/or closely monitored to dedicated portals accounting for national differences and providing targeted advice to law enforcement authorities.
    - These practical measures have resulted in significant improvements of the direct cooperation between those service providers and law enforcement authorities, in terms of reliability, quality and efficiency. Nevertheless, not all service providers have implemented these measures and more could be done to ensure a common approach amongst service providers.

2) **Streamline procedures** on both the public authorities' and the service providers' side:
    - On the **public authorities' side,** the **standardisation and reduction of forms** used by law enforcement and judicial authorities could facilitate the creation of requests by law enforcement and increase the confidence of service providers when it comes to the identification of authorities and proper forms used.
        - Some Member States (FR, HU, SE) have already cooperated with service providers to create and implement such forms, taking into account the requirements from a national criminal procedural law perspective and

from the service provider's perspective, e.g. as based on applicable law of other related countries.
    - This has resulted in the improvement of the functioning of this channel and, in some cases, in a significant reduction in the number of forms used.
    - Depending on the specific requirements of the national criminal procedural law and the different business models and infrastructures used by service providers, forms could be developed to allow for harmonised law enforcement input to service providers.
    - The Commission could facilitate the development of these standardised forms by national authorities and service providers on a voluntary basis.
- On the **service providers' side,** significant improvements could be made through **streamlining service providers' policies** to reduce the heterogeneity of approaches, notably regarding procedures and conditions for granting access to the requested data.
    - Given that there is no legal framework in place, currently all service providers are free to choose whether and on what terms they provide access to non-content data. The development and application of harmonised procedures, standards and conditions (e.g. where specific data categories common to several providers are concerned) could facilitate direct cooperation between public authorities and service providers.
    - A harmonisation of procedures, standards and conditions could bring unity in current approaches that sometimes appear to differ widely. This would reduce the challenge that public authorities currently face to understand and work with the different policies and procedures and keep up with changes and new developments, possibly leading to a more efficient process when preparing the requests at the side of law enforcement authorities.
    - Although the various infrastructures and very different business models used by service providers may not allow for a full harmonisation of policies, the Commission could further explore streamlining opportunities with service providers on a voluntary basis.

3) **Provide opportunities for the exchange of best practice and training** of public authorities in the EU on cooperation with US-based providers.
- All stakeholders indicated that additional **training for law enforcement and judicial authorities** could support the functioning of direct cooperation between those authorities and service providers.
    - Training activities could provide for a better understanding of different policies and procedures used by service providers. A common understanding of other countries' law concepts and technical capabilities might enhance responses.
    - Experts suggested that training should not be fragmented per country but could rather be centralised to ensure for synergies.

- The Commission could facilitate the development of training programmes in full collaboration with national authorities and service providers on a voluntary basis. The Commission has made available **EUR 500 000** under the Partnership Instrument [250] for improving direct cooperation with service providers.

- Several stakeholders suggested the **establishment of an online information and support portal** at EU level to provide support to investigations, including information on applicable rules and procedures.

  Possible uses of the platform could range from a static repository for service provider policies to an interactive tool guiding law enforcement authorities in identification of the relevant service provider and appropriate channels to use, to a comprehensive tool allowing for the creation and submission of requests to several service providers.

  It could leverage the work of existing initiatives which already pursue similar objectives, including:

  - efforts under the **Council of Europe Budapest Convention on Cybercrime** to create a static repository of the different provider policies and information on criminal procedural law of States Parties to the Budapest Convention[251];
  - other repositories of service provider policies[252]; and
  - Europol's **SIRIUS platform** to facilitate online investigations, including the direct cooperation between authorities and service providers[253].

Where relevant, these practical measures on direct cooperation with service providers on a voluntary basis for non-content requests could be developed and implemented in the context of the existing EU Internet Forum[254].

**Legislative action**

Measure 3: multilateral international agreements

---

250 The Commission launched a call for proposals with a budget of EUR 1million total for improving cooperation both between judicial authorities of EU Member States and the US and between EU authorities and US-based service providers on 4 May 2017 under the Partnership Instrument Annual Action Programme 2016 Phase II - International Digital Cooperation - Component D – Cross Border Access to Electronic Evidence (EuropeAid/155907/DH/ACT/Multi). More information is available here.

251 See T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, T-CY (2016)5 provisional, 16 September 2016 and the Abridged meeting report of the 14-15 November 2016 Council of Europe T-CY 16th plenary meeting, T-CY (2016)32 of 15 November 2016.

252 See e.g.: the Search.org ISP List database, which provides contact information and instructions needed to serve judicial process (US domestic) on a number of US-based or headquartered service providers.

253 This interactive platform would allow law enforcement authorities to collect publicly available information, to identify the relevant service providers for additional information, and to find the appropriate channel for making the request. More information is available here.

254 The EU Internet forum is an initiative of the European Commission that brings together EU Interior Ministers, high-level representatives of major internet companies, Europol, the EU Counter Terrorism Coordinator and the European Parliament. Its goal is to reach a joint, voluntary approach based on a public-private partnership to detect and address harmful material online. More information is available here and here.

This measure would seek to address problem drivers 1 and 3 by reducing the need for judicial cooperation and clarifying jurisdiction for investigative measures.

Multilateral international agreements ideally create a common framework across a wide number of countries affected by the same challenge. In the field of cyber-enabled crime, the 2001 Council of Europe Convention on Cybercrime (the Budapest Convention) is the main multilateral framework, providing harmonised definitions and procedural rules, as also recognised in the 2013 EU Cybersecurity Strategy[255]. The Budapest Convention is well placed as an international agreement to address the challenges to cross-border access to e-evidence. However, as of now, the Convention only addresses specific smaller parts of this topic as no wider agreement could be reached when the Convention was negotiated almost 20 years ago.

Accession to the Budapest Convention is open to member countries of the Council of Europe, and also to other countries, based on an invitation extended after a unanimous decision of all Parties to the Convention. Currently, 55 countries have ratified the Convention, including all Member States except Ireland and Sweden, which have signed the Convention and are in the process of ratification through implementation in national law. The EU is not a party to the Convention but is committed to promoting it. The European Commission takes part in plenary meetings of the Convention Committee (T-CY) as an Observer Organisation. Important Parties to the Convention from beyond the EU are the US, Japan and Canada. An increasing number of countries are taking steps in view of ratification or accession to the Convention.

At its 7-9 June 2017 plenary meeting, the T-CY adopted Terms of Reference for the negotiation of an Additional Protocol to the Convention between September 2017 and September 2019[256]. The scope may expand the existing framework allowing for **direct cooperation** with service providers in other jurisdictions (possibly including subscriber information, preservation requests, and emergency requests), as well as create a **clear framework and safeguards** (including data protection requirements) for cross-border access to information.

In terms of **timing**, if negotiations are indeed concluded by the end of 2019, the protocol would then need to be ratified by the parties that want to adopt it, which may take several years. If an e-evidence legislative proposal is adopted by the Commission and negotiated and adopted by the EU legislators before the end of 2018, then it is likely that the EU e-evidence instrument might come into effect before the protocol.

In terms of **scope**, the protocol will be wider, also tackling issues such as language regimes or the use of video conferences for mutual legal assistance among the parties to the Convention. However, for the specific aspects tackled by the preferred option of the present initiative on e-

[255] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace (JOIN(2013) 1 final of 7.2.2013).

[256] (DRAFT) Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, T-CY (2017)3, version 1 June 2017.

evidence, it is expected that the protocol a) will not be as far-reaching as it is not based on the same level of mutual trust among the more diverse 50+ parties to the Convention and b) will lack the enforcement mechanisms that EU law has, as it is an international Convention with no compliance mechanisms beyond discussions between the parties. While we expect that the protocol and the present initiative will be coherent, compatible and mutually reinforce one another, thanks to a coordinated position of Member States, for these reasons we also expect to see a more effective and more far-reaching cooperation on cross-border access to e-evidence among EU Member States.

Therefore, the interest for the EU to participate in the negotiation of this Additional Protocol is threefold:

3) Some non-EU countries which are also Parties to the Budapest Convention (e.g. the US) are very important in improving cross-border access to e-evidence.
4) While the scope is unlikely to extend to content data, it may include elements that are already covered by existing acquis at EU level, including on Mutual Legal Assistance or in relation to the European Investigation Order.
5) It may help address some of the **reciprocity** issues that a possible EU legislative initiative could generate (see option C, in particular Box 5).

The negotiations will be prepared by a smaller drafting group, which is only open to State Parties. A first meeting of the drafting group took place on 19-20 September 2017. The Commission attended the meeting in expert capacity, as appointed by the T-CY.

The negotiations of the Additional Protocol are closely linked with a possible proposal on e-evidence: if a proposal is made, consistency will have to be ensured, and there will also be a clear competency for the EU and obligation for the Member States to defend a common position. The most appropriate way to ensure compatibility of the second Additional Protocol with existing and possible future EU acquis is for the Union to participate in the negotiations, following the procedure established in Article 218 TFEU[257]. The negotiation could be conducted by the Commission insofar as matters under shared or exclusive EU competence were concerned, whereas if the Protocol covered both EU competences and sole national competences, special negotiating arrangements should be agreed between Commission and Council. The resulting instrument would be signed by EU Member States and could be ratified by them once they had adopted the necessary legislation to comply with the international obligations stemming from it.

The large group of parties of the Budapest Convention is an advantage and a disadvantage in this context. It is an advantage insofar as any common solution applies to a large number of partner countries of the EU. The downside of the large number of parties lies in the smaller common denominator that exists across a diverse group such as this one. This may create a risk for the drafting process and may also result in a reduced scope of any such protocol. In any case, it appears evident that the new protocol, while certainly helpful beyond the EU, would not be able to match the level of integration within the EU because of a lack of a

[257] Consolidated version of the Treaty on the Functioning of the European Union – Part five, External Action by the Union – Title IV: Restrictive Measures – Article 218 (ex Article 300 TEC).

common and harmonised framework of safeguards across all the countries that are party to the Budapest Convention.

## ANNEX 8: ADDITIONAL INFORMATION ON EARLY DISCARDED MEASURES

The following policy measures were considered at an early stage but subsequently discarded:

1) Non legislative action.
   - Practical measures to enhance judicial cooperation among public authorities and direct cooperation between public authorities and service providers.
     - Within the EU:
       - Develop a **platform** to centralise the communication between service providers and public authorities across the EU.
         This measure was discarded as it was considered more feasible to first develop a platform for public authorities only and then possibly open it to service providers (and likely also public authorities of non-EU countries) as well.
       - Facilitate coordination of **service providers** to achieve **full harmonisation** of policies, standards and forms to provide access to public authorities to e-evidence.
         This measure was discarded due to the opposition of service providers, as they have very different procedures and types of data available that would have made the implementation of this practical measure on a voluntary basis unfeasible.
       - Leverage **ETSI (European Telecommunications Standards Institute) standards** for lawful interception in telecommunications to facilitate the interactions between public authorities and service providers across the EU with regard to the access to e-evidence.
         This measure was discarded due to the opposition of service providers, as it would also imply standardising their very different procedures with regard to the different kinds of data their services generate, depending on their business models.
     - Modify the **EIO form** contained in the annex to the EIO Directive to adapt it better to the needs of cross-border access to e-evidence.
       This measure was discarded because it would imply changing the EIO Directive, where the forms are included as annexes. The EIO Directive became applicable very recently (May 2017) and was the result of difficult negotiations. Therefore, there are no plans to reopen negotiations of this instrument before it has reached its full potential and has been fully implemented by Member States, as this could be too disruptive for Member States.
     - With non-EU countries:
       - Develop a common online **form**[258] for MLAT requests to the US which could help public authorities in Member States to better comply with US

[258] The President's Review Group on Intelligence and Communications Technologies already highlighted in 2013the possible convenience of creating an online submission form for MLATs to streamline the process, Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, December 12, 2013.

requirements, in particular with regard to probable cause in the requests for content.

This measure was discarded due to the opposition of US authorities who are of the view that such a form can only provide a part of the solution. In particular, it would not solve the major issue faced by EU practitioners concerning the demonstration of probable cause, for which trainings and guidance may be more adapted than standardisation. The possibility to standardise the probable cause requirement is very limited as the demonstration has to be done case by case and, in application of the US common law legal framework, part of the relevance of the demonstration depends on the jurisprudence of each judge.

Rather than focusing on developing a common online form for MLAT, US authorities also indicated that Member States should also consider and implement other permissible ways of accessing evidence which do not require mutual legal assistance.

2) Legislative action.

- Legislative measure on **judicial cooperation**: **amend the EIO Directive** to include provisions on e-evidence
  - For the reasons set out in Annex 4, section 1 (Legislative action: direct cooperation, Measure 5: European Production Order), it is more appropriate to create a new instrument than to amend the EIO to include provisions on electronic evidence.
- Legislative measures on **judicial cooperation**: **international agreements**.
  - Promote a new **United Nations convention** on cross-border access to e-evidence, which would replace the Council of Europe Convention on Cybercrime.

    This measure was discarded as the Council of Europe Convention on Cybercrime is already open to all countries and is the instrument of choice as per long-standing EU policy. In addition, it is unclear whether the level of safeguards that would likely be put in place at UN level would suffice to protect fundamental rights as they are understood in the EU, given the significantly different definitions of cybercrime in various non-EU countries.
- Legislative measures on **direct cooperation** with service providers.
  - Introduce mandatory **data localisation**, i.e. require service providers offering services in the EU to store their data in the EU.

    This measure was discarded as it would contribute to the fragmentation of the Internet and could have negative economic consequences on EU companies as they trade globally[259]. Although it might provide an easy solution at first view, this obligation would be more far reaching for service providers as it could trigger important changes to the way they store their data and would imply higher costs. Depending on its scope, it could be viewed as a trade barrier.

[259] The International Communications Privacy Act, recently proposed in the US Senate as previously discussed, uses similar arguments against data localisation. In particular, Sec.5 specifies that: "The data localization requirements imposed by foreign governments on data providers are (A) incompatible with the borderless nature of the Internet; (B) an impediment to online innovation; and (C) unnecessary to meet the needs of law enforcement".

- Restrict the **scope** of the legislation to **data stored in the EU**.
  This measure was discarded since, as described in section 2 (problem definition, see figure 1), e-evidence can be located in or outside the EU for reasons unrelated to the user and/or public interests, it can be volatile (i.e. it can change location rapidly, inside and outside the EU), it can be split in multiple countries or its location can be simply unknown. In other words, data storage normally takes place outside the control of the state on whose territory data is stored. Therefore, the only way for a Member State to ensure that data is stored in its territory would be through data localisation requirements (see above).
- Include an **obligation** to provide data from **live intercept**.
  This measure was discarded because while such obligations exist in most national laws for the domestic setting, they are usually tightly restricted and subject to additional safeguards, as live intercept can give access to more sensitive information on the target. For certain countries including the US, live intercept cannot be asked by way of MLA request.
- Introduce an **obligation** for service providers **to decrypt encrypted data** before giving access to public authorities to e-evidence.
  This measure was discarded since the use of encryption is essential to ensure cybersecurity and the protection of personal data (EU legislation specifically notes the role of encryption in ensuring appropriate security for the processing of personal data [260]) [261]. Solutions that intentionally weaken technical protection mechanisms to support law enforcement (e.g. so called "backdoors) would intrinsically weaken the protection against criminals as well[262].
- Limit the **scope** of application of the European Production Order to **certain crimes** (e.g. serious crimes).
  This measure was discarded because:
    - limiting the scope of the request to certain categories of crimes (e.g. according to maximum sentencing or through the use of a list) may reduce the effectiveness of the investigation for those crimes not covered, as the traditional judicial cooperation procedures may be too slow to secure the data in time, especially in the absence of data retention schemes. In particular, the impact of certain high-volume, low-impact offences (e.g. online and card payment fraud), which could be seen individually as less serious but collectively cause significant damage to citizens, should not be underestimated. Excluding them here could essentially render them more difficult to investigate at all. The same is true for offences that can only be

[260] See Article 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[261] Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union, COM(2017) 608 final, 18 October 2017.

[262] Europol and ENISA Joint Statement, On lawful criminal investigation that respects 21st Century data protection, 20 May 2016.

committed by electronic means such as cybercrime or fraud in non-cash means of payment, which are not necessarily serious crimes, but for which the evidence will typically exist only in electronic form;

- limiting the scope could have a positive impact on proportionality and fundamental rights as it would limit the measure to situations where the seriousness of the offence warrants a comprehensive investigation using all tools available. However, when compared to other investigative tools, a production order is a relatively low-impact measure, in particular when it comes to subscriber data, access logs or similar information. The more significant potential impact that a larger scope could have on fundamental rights would be balanced by considerations of effectiveness, provided that detailed conditions and safeguards are set;
- besides effectiveness considerations, a large scope would also not impose a significantly higher burden on service providers, as – if the EPO were to be limited to serious crimes – MLA or EIO channels would then have to be used for the remaining requests, which would also result in the same service provider having to provide the data.

- Use as a **connecting factor** to exercise jurisdiction:
  - the **accessibility of the service** (e.g. web site or app) from the EU.
    This measure was discarded as it would result in a very wide scope that might be disproportionate in relation to the burden imposed on the service provider. As most service providers do not geographically restrict their online presence, almost any service is available from within the EU and would be in scope if this connecting factor was used;
  - the **pure corporate presence** in the EU of a service provider.
    This measure was discarded as it would create a competitive disadvantage to companies with various business activities (those of a service provider and others), operating in the EU compared to those only with business activities of a service provider;
  - the **nationality of the suspect.** Some of the service providers currently use this criterion to decide whether to cooperate voluntary with foreign public authorities (e.g. a service provider only facilitates access to e-evidence to Italian law enforcement if it concerns Italian nationals).
    This measure was discarded as investigations by Member States are not limited to certain nationalities and such restrictions would undermine the effectiveness of accessing e-evidence across borders; and
  - any factor susceptible to be shaped by **internal company policies**.
    This measure was discarded as it would leave the effectiveness of law enforcement in the hands of company policy, placing service providers in a difficult position.
- Use as a criterion to require service providers to designate a **legal representative** in the EU that the service has at least **1 million users** in the EU.
  This measure was discarded because besides not having a solid foundation concerning the specific threshold of 1 Million (i.e. why not 500,000 or 2 Million?)

and the difficulty to apply it in practice (as it might not be possible to determine the number of users a service provider has in the EU, the number of users can fluctuate rapidly), it would create a gap that could easily be exploited by criminals and would seriously undermine the effectiveness of the measure.

- Oblige service providers to nominate **a legal representative in every Member State** in which they are active or which they are targeting.
  This measure was discarded as being too burdensome on service providers. Furthermore, given that a European Production Order or Request could be served across EU internal borders, it did not seem necessary. The administrative burden this would create for the service provider would not be outweighed by the additional facilitation this would provide.
- Allow to address an EPO to **any corporate presence** of the service provider in the EU, without requiring service providers to nominate a legal representative in such cases.
  This measure was discarded, as the example of the Apple Store shows that not every corporate presence would be equipped with the capacity to respond to an EPO. Service providers need a say in who should be the addressee of such EPOs.
- **Rely on non-EU countries** for service of orders to service providers established in those countries.
  This measure was discarded as it would greatly diminish the effectiveness of the instrument in particular as regards the EPO; an EPO that cannot be served directly would essentially remain voluntary in nature unless accepted through mutual recognition or legal assistance mechanisms.
- Enter into an **agreement with the US** to allow service of documents directly in the US on US-based service providers.
  This measure was discarded as this is currently not provided for under US law and would require a change of laws. In addition, it is unlikely that the US would accept this as the legislation that is currently under negotiation to enable a US-UK agreement on direct cooperation for content data expressly excludes granting a binding nature to the request. For the serving of documents, such an agreement would offer no material change from the current situation, where service providers already have channels available for authorities to share legal process with them, while not recognising any binding nature of the requests and preserving their right to fulfil the request only if they so choose.
- Use under the EPO a **notification system** to the receiving State (where the service provider is located) with the right to object within 96 hours.
    - This system would be comparable to the one in the **EIO** (Article 31). Judicial authorities would send a European Production Order to the service provider and a notification with a short description of the case (not more than in an EIO) to the "receiving" State. This would not prevent the service provider to provide the data to the issuing State but the evidence would not be used for further investigation or in the trial if the receiving State objects.

This measure was discarded because such a notification system would generate significant bureaucratic **burden** for the issuing and the receiving States:

- The issuing State would have to fill in different **forms** and would have to **translate** additional information for the receiving country as it would need to provide details that the service provider has no right to see.
- The receiving State would receive notifications from at least **24 other Member States** which would need to be checked. Some Member States with many service providers on their territory (e.g. Ireland, provided that they opt in the EPO) would receive more notifications than others, most of which would concern cases or suspects unrelated to the State in which the service provider is located. Given that Member States have specifically given a mandate to the Commission to come up with a direct production order, this did not match that ambition as it would essentially recreate the EIO with a more burdensome approach for receiving Member States because of the necessarily very short deadlines.

- A production **request for non-content data and a production order for content data.**
  This measure was discarded as it would not be consistent to use a more intrusive measure, the production order, for data that is less intrusive, and vice-versa.

- Legislative measures on **direct access** to electronic evidence.
  - Set up an **EU legal basis** for direct access to electronic evidence.
    This measure was discarded as very heterogeneous approaches currently exist across EU Member States to these issues and it seemed unlikely that a common basis could be established. Those Member States which already have more advanced solutions in place appeared firmly convinced of the necessity of preserving the scope of their national measures and their current capabilities, and some of those who have restrictive solutions in place at the moment were reluctant to change their approach.
  - Harmonise at EU level **search and seizure** measures.
    This measure was discarded because it would go beyond what is necessary to address the issue at hand, i.e. remote access to stored data.
  - Restrict the scope of the legislation to service providers with a given **connection to the EU**.
    This measure was discarded as direct access is often used in situations where there is no (legitimate) service provider, where it is not possible to locate the service provider or where it is unknown, and therefore its connection with the EU would be unknown.
  - Restrict the scope of the legislation to data stored in the EU (i.e. **data storage** requirements).

This measure was discarded for the same reasons described above under direct cooperation.

- Introduce **mandatory notification** to the **public authorities** of the country of habitual residence of the target of the measure by the public authorities of the Member State carrying out the measure.
  - This measure, modelled on Article 31 of the EIO Directive ("Notification of the Member State where the subject of the interception is located from which no technical assistance is needed"), would grant the receiving country the opportunity to object[263].
  - The habitual residence is typically the location where the user regularly exercises control over the data. Also, the State of habitual residence has the responsibility to protect the basic rights of its citizens and of those persons who have their lawful and permanent residence there.
  - Such a solution could provide information about the extent to which the Member State recurs to direct access to data of its permanent residents. It could also prevent situations where an investigation in the Member State carrying out the measure could interfere with an ongoing investigation in the other country.
  - However, there are a number of drawbacks that caused this measure to be discarded:
    - Such a notification system would create a fully new procedure and an administrative burden on the receiving country which might not have a specific interest to intervene. In particular, some notification obligations already exist when prosecuting a foreign national, and there are also coordination mechanisms for possible parallel investigations, so it did not seem necessary to create an additional notification trigger. Often it will not yet be evident whether an investigation will proceed or even go to trial eventually; in this case, the involvement of the country of the target might not be useful.
    - The notification to the country of the target's residence furthermore fails to address the possible sovereignty considerations that the state of data storage could raise if it attaches importance to data storage location.
    - In addition, it would be difficult to reconcile the mandatory notification with a possible need to delay user notification, as the notified country would have little chance to take a position in the absence of contact with its resident.
  - Furthermore, it would create challenges when a non-EU country would need to be notified: national experts expressed a preference to forego a notification in such cases.

[263] This option was presented by Germany during the expert process and discussed with the other Member States (see Annex 2).

- Introduce **mandatory notification** to the **public authorities** of the country where the data is stored.
    - This measure would address the possible sovereignty considerations that the state of data storage could raise if it attaches importance to data storage location.
    - This measure was discarded during the expert process, where it was identified as unrealistic:
        - One of the main situations in which direct access is currently used is in "loss of knowledge of location" situations where authorities cannot determine the data location in good time. Often, when conducting the investigation, the data location remains hidden, e.g. when the server accessed is using relay infrastructures such as The Onion Router (TOR). Therefore, such a notification obligation would remain mostly theoretical in nature.
        - On the other hand, if authorities were compelled to identify the location – which is often irrelevant for the investigation, e.g. if the location of the target is known already – it could lead them to take additional investigative steps when accessing the data that are not necessary to contribute to resolving the case. Such a notification obligation could therefore create an incentive for a more intrusive access, which would run counter to the purpose of such a safeguard.
        - It was also unclear what benefit the notified state would derive from the notification, other than the awareness that data on its territory was accessed. As the storing of data on its territory takes place without the agreement or even awareness of the country, the added value of being informed about the access appeared limited.
        - In addition, it did not comply with the logic of the proposal to move away from data storage location as a decisive factor.

## ANNEX 9: ADDITIONAL INFORMATION ON THE BASELINE

The baseline or **option O** is the scenario in which there is **no EU action**. This scenario has several dimensions:

1) **In general** terms, the problem drivers are likely to evolve as described in section 2.3. (How will the problem evolve), worsening the situation.
   - **Judicial cooperation** would likely take longer, given the exponential growth of electronic data and the increase in requests due to the loss of publicly available data, which is unlikely to be matched by a growth in resources to deal with the increased number of MLAT/EIO requests.
   - Without a clear framework for **direct cooperation** between service providers and public authorities:
     - the efficiency of this cooperation is, similarly, likely to decrease under the strain of the ever increasing number of requests. In addition, the sheer growth in volume of direct requests might create a disincentive for new or continued cooperation;
     - in the absence of a clear **legal basis**, law enforcement may be unable to make requests for direct cooperation that are in compliance with Directive (EU) 2016/680 (the "Police Directive" or the **data protection** directive for law enforcement)[264] and in particular with Article 39, which sets specific conditions for such requests;
     - for data that is publicly available at present but will move into gated-access systems by May 2018 (e.g. WHOIS), when the new data protection framework comes into effect, availability to law enforcement will cease, absent a specific legal basis to address the data protection and criminal procedural law requirements.
   - Without a clear EU framework defining **jurisdiction** in cross-border access to e-evidence, Member States are likely to introduce different practices and legislative instruments at national level which would lead to **fragmentation** and hamper effective cross-border cooperation in investigations and prosecutions. This would also further exacerbate the challenges service providers already face in assessing many different legal systems and may adversely affect the willingness of service providers to continue to invest in cooperation in which they are not obliged to participate.

[264] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

2) **Existing and incoming EU legislation** is not likely to effectively address the challenges in cross-border access to e-evidence, in the absence of specific EU action to address those challenges in each of the channels:
   - **Judicial cooperation** challenges:
     - The **EIO Directive** is the main legal instrument to gather and transfer evidence between Member States. As explained in the problem definition (section 2.2.1.), it was not conceived for the specific purpose of cross-border access to e-evidence, and it has a number of drawbacks. These include the deadline of 120 days to respond to provide access to e-evidence, which is still considered too long for an effective access to that type of evidence in criminal investigations. Shorter deadlines that are provided by the EIO Directive for urgent cases cannot address the specific needs of e-evidence with its high relevance for criminal investigations: it is an exception rather than the general rule, requiring reasons for urgency in every case.
     - That said, there is room to improve the expediency of judicial cooperation in the EIO through a set of non-legislative initiatives at EU level (see option A below). In the absence of EU action, these improvements would not take place.
     - In addition, Ireland and Denmark do not participate in the EIO, and will continue to rely on MLA channels for accessing electronic evidence in another Member State, with no legal deadlines to access e-evidence.
     - Furthermore, the EIO does not resolve the challenges in accessing evidence held by service providers headquartered outside the EU, as this dimension is outside its scope, and it does not address the issue of data available using a login and password as this issue had not yet arisen at the time of the EIO drafting and negotiation.
   - **Direct cooperation** challenges:
     - As described in the legislative context (section 1), a number of proposals under discussion in different areas touch upon various aspects of access to e-evidence. These include the, the proposal for a Regulation on a framework for the **free flow of non-personal data** in the EU and the proposal for a Directive **to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market.** In addition, the **Proposal for a Regulation on Privacy and Electronic Communications** provides that Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of the General Data Protection Regulation. Although these proposals touch upon related issues to the problem of cross-border access to e-evidence, none of them specifically

focuses on tackling that problem, leaving a large number of issues in criminal investigations unaddressed or up to sector-specific legislation. Nonetheless, these proposals should be taken into account in this initiative to ensure coherence.

- **Direct access** challenges:
    - There is no current or incoming EU legislation addressing the challenges of direct access to e-evidence.

3) **International agreements** between Member States and non-EU countries are likely to evolve in an uncoordinated way without EU action.
    - Council of Europe Convention on Cybercrime.
      A negotiation was launched in 2017 to add a new protocol to the Convention. The protocol could include:
        - provisions for more effective mutual legal assistance;
        - provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests and emergency requests;
        - a clearer framework and stronger safeguards for existing practices of trans border access to data, and
        - safeguards, including data protection requirements.

      These negotiations will go ahead regardless of whether the EU acts. In the absence of EU action (i.e. active participation in the negotiations, ensuring coordination among Member States), the strength of a coordinated negotiating position would be lost, possibly with suboptimal consequences for Member States. If the EU adopts its own legislative proposal on cross-border access to electronic evidence, the need for an active participation becomes even more evident as coherence between EU law and the Convention should be ensured. Otherwise Member States might be forced to choose between compliance with either the new protocol of the Convention or the new EU legal framework.
    - Bilateral agreements
        - The problem definition (section 2) showed the **limitations** of the current MLA Treaties used to access e-evidence across borders.
        - To address some of the issues concerning the MLA procedure with the US, the DOJ/OIA organises **trainings** for practitioners in the requesting countries on understanding US legal standards and on how to fill the MLAT application in correctly. In addition, the **liaison magistrates** of the Member States to the US have significant operational experience in the MLAT process and play a key role in facilitating the communication between the Member States and the DOJ. In particular, they prepare guidelines to the judges in their Member State on how to prepare MLAT requests and the MLAT procedure.
          That said, these operational improvements are not likely to bring substantial improvement to the current procedures.
        - From the perspective of US law there is no need to go through the MLA process for **non-content** data. As a result, it is difficult to justify to the US

authorities why they should continue investing resources in a procedure that is superfluous from their perspective.

- Judicial cooperation between public authorities through the MLA process could also be influenced by the decision of the US Supreme Court on the **Microsoft Ireland case**, expected by July 2018. The DOJ had previously sought access to content data from service providers in the US (also on behalf of requesting EU Member States) regardless of where it was stored. Microsoft challenged this practice in 2013 (see box below). The US Supreme Court could allow US law enforcement to continue to request US service providers access to e-evidence regardless of where it is stored (including evidence stored in the EU), or could limit US competence, forcing a change in legislation. Without coordinated EU action in preparation for the possible outcomes of this case, Member States would be exposed to its consequences in different ways, which could generate different responses from them and lead to fragmentation and hampered cross-border cooperation.

*Box 1: the Microsoft Ireland case*

In 2013, Microsoft challenged a warrant by US law enforcement to turn over email of a target account that was stored in Ireland, arguing that a warrant issued under Stored Communications Act (part of ECPA) could not compel American companies to produce data stored in servers outside the US.

Microsoft initially **lost** in the **New York District Court**, with the judge stating that the nature of the Stored Communication Act warrant, as passed in 1986, was not subject to territorial limitations.

Microsoft appealed to the United States Court of Appeals for the **Second Circuit**, which **agreed** with Microsoft and invalidated the warrant. The United States Department of Justice counter-appealed to the **Supreme Court**, which agreed to hear the case in October 2017.

In other similar cases, Courts outside the 2nd Circuit's jurisdiction have ordered companies to comply with warrants if they can access the data from within the United States, regardless of where the data is stored[265].

In response to the Microsoft case, a number of legislative proposals have been put forward, including a **DOJ proposal** (see box below) affirming

[265] See for example a case with Google, Orin Kerr, Google must turn over foreign-stored emails pursuant to a warrant, court rules, The Washington Post, 3 February 2017.

the position that data can be requested regardless of storage location and the **International Communications Privacy Act (ICPA)**[266], a bipartisan proposal that aims to clarify US law enforcement's ability to obtain e-evidence while respecting privacy laws of other countries. The ICPA proposal has been welcomed by service providers[267].

*Box 2: DOJ draft legislation of cross-border access to e-evidence*[268]

In July 2016[269] and May 2017[270], the DOJ proposed legislation to address some of the limitations of the current MLAT process. The proposal, which takes into account previous papers and working group efforts[271], moves away from the current MLAT system. Instead, the new legislation would:

2) allow **bilateral agreements** on this issue between the US and participating countries; and
3) allow the countries that have been approved for these bilateral agreements to **submit requests** for electronic data (both stored and intercepted live), **directly to US service providers**, instead of first going through US courts.

The draft DOJ legislation sets out the standards countries must meet to qualify for an agreement and establishes parameters on what the requests can include. For instance, requests must pertain to a **serious crime**, including terrorism. This proposal would also afford the US **reciprocal rights** with respect to the partner country. More details on the proposal, including possible benefits and concerns are available in Annex 10.

266 S.1671 - International Communications Privacy Act, previously also introduced in the U.S. Congress.

267 Orrin Hatch, Tech Leaders Praise Hatch/Coons International Communications Privacy Act, 1 August 2017.

268 Lin, Tiffany and Fidler, Mailyn, Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement, Berkman Klein Center Research Publication No. 2017-7, Harvard University, September 2017. On 23 March 2018 the US Congress adopted the Clarifying Lawful Overseas Use of Data (CLOUD) Act, right before the adoption of the EU legislative proposals that this impact assessment accompanies. The CLOUD Act is available here.

269 U.S. Department of Justice, Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism, July 15, 2016.

270 Statement of Richard W. Downing, Acting Deputy Assistant Attorney General, Department of Justice, before the Committee of the Judiciary, U.S. House of Representatives, for a hearing entitled "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era", June 15, 2017. The proposal was submitted again in 2017 as the US Congress changed in the November 2016 elections.

271 See for example:

- Jennifer Daskal and Andrew K. Woods, Cross-Border Data Requests: A Proposed Framework, Just Security, November 24, 2015;
- Peter Swire and Justin D. Hemmings, Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program, NYU Annual Survey of American Law, vol. 71 (2017), pp.687-800;
- Greg Nojeim, MLAT Reform: A Straw Man Proposal, Center for Democracy & Technology, Sept. 3, 2015.

- In the absence of EU action, the current MLATs between the EU and non-EU countries would not be updated. In this scenario, Member States would likely be inclined to update or sign new bilateral agreements with non-EU countries, in particular with the US, to expand direct cooperation possibilities, leading to **fragmentation** that may hamper international cooperation in investigations and prosecutions. Member States themselves have expressed during the consultations the desire to avoid such a country-by-country approach if possible.
- The recently **proposed legislation by the DOJ** may contribute to that fragmentation. The **UK** has already started negotiations for a UK-US agreement that would allow it to be the first country approved to make requests under this new legislation. Other Member States could follow, notably in the absence of EU action.
- Additionally, as outlined above, the US is taking steps to reduce the relevance of the MLAT procedure and privilege other channels. The EU and its Member States need to respond to this shift by creating the necessary legislative tools to utilise those other channels.

6) **Direct cooperation** between service providers and public authorities could evolve in a wide range of possible ways, none of which the EU would have the opportunity to shape and contribute to in the absence of EU action.
   - The **DOJ proposal**, if converted into law, would have implications on the direct cooperation with service providers. That said, it is unclear if and when and in what final form the proposal would become law[272]. Without coordinated EU action, US law would continue to determine global practices and Member States might enter different bilateral agreements with the US that might lead to fragmentation and hamper cross-border cooperation in the EU.
   - The decision of the US Supreme Court on the **Microsoft Ireland case** could also shape the direct cooperation between public authorities and service providers in the coming years. Specifically, a ruling in favour of US public authorities having access to content data from service providers in the US regardless of where it was stored could put service providers in a situation of conflict of laws, between privacy laws of the country where the evidence is stored and US search warrants. Again, without coordinated EU action, US law would continue to determine global practices, which could also affect the current direct cooperation on a voluntary basis.

7) **Direct access** to electronic evidence could increase, as Member States could introduce new legislative and non-legislative initiatives on direct access, possibly increasing fragmentation and hampering cross-border cooperation.

[272] On 23 March 2018 the US Congress adopted the Clarifying Lawful Overseas Use of Data (CLOUD) Act, right before the adoption of the EU legislative proposals that this impact assessment accompanies. The CLOUD Act is available here.

As the need to access e-evidence across borders increases and the judicial and direct cooperation methods may become more and more inadequate to provide effective responses, Member States may turn to other methods to facilitate access to e-evidence directly. These could include initiatives such as data localisation requirements[273], limitation in the use of encryption[274], or other methods which might not offer uniform safeguards across the EU and would hamper cross-border cooperation.

In summary, the baseline scenario not only falls short in addressing the concerns expressed by stakeholders, but in the absence of EU action those concerns are likely to increase as the situation worsens across multiple dimensions.

[273] See Stephen Dockery, Data Localization Takes Off as Regulation Uncertainty Continues, The Wall Street Journal, 6 June 2016.

[274] See e.g., Jenny Gross and Alexis Flynn, U.K. Proposal Would Expand Government's Power of Surveillance, The Wall Street Journal, November 4, 2015;
Rachel Pick, A Look at France's New Surveillance Laws in Wake of the Paris Attacks, Vice – Motherboard, 15 November 2015.

## ANNEX 10: US DOJ PROPOSAL ON CROSS-BORDER ACCESS TO E-EVIDENCE

This annex[275] summarises the content of the US DOJ proposal[276] and lists a number of benefits and concerns stated by stakeholders.

Details of the proposed legislation

The proposal amends parts of ECPA such as the Stored Communications Act and the Wiretap Act. It outlines conditions a foreign government must meet to qualify for an executive agreement with the US[277] The Attorney General, with the concurrence of the Secretary of State, must determine and certify to Congress that the foreign government meets certain standards, including that the foreign government has domestic laws that afford robust substantive and procedural protections for privacy and civil liberties. These conditions require, in part, that the foreign government has:

- substantive and procedural laws on cybercrime and electronic evidence;
- evidence of respect for the rule of law and principles of non-discrimination, and
- adherence to applicable international human rights obligations;
- mechanisms to provide accountability and transparency for data collection;
- a showing of clear mandates, procedures, and effective oversight of authorities' collection, retention, use, and sharing of data;
- mechanisms for accountability and transparency for the collection and use of data; and
- a commitment to promote and protect the free flow of information and the open Internet (essentially a promise not to pursue actions such as data localisation).

Once a country has established an executive agreement, that country is able to send a request to an electronic communications company directly, without first going through US agencies or courts. The request itself:

- cannot infringe freedom of speech;
- must be subject to review or oversight by a court, judge, magistrate, or other independent authority in the issuing country;
- must be based on requirements for a reasonable justification based on articulable and credible facts;
- must be issued in compliance with the foreign country's domestic law, and any obligation for a provider to produce data is solely from that law;
- not intentionally target a US person (or person located in the US) or target a non-US person with the intention of obtaining information on a US person;

---

[275] Lin, Tiffany and Fidler, Mailyn, Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement, Berkman Klein Center Research Publication No. 2017-7, Harvard University, September 2017.

[276] U.S. Department of Justice, Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism, July 15, 2016.
On 23 March 2018 the US Congress adopted the Clarifying Lawful Overseas Use of Data (CLOUD) Act, right before the adoption of the EU legislative proposals that this impact assessment accompanies. The CLOUD Act is available here.

[277] *Ibid.*, §4(a).

- must pertain to the "prevention, detection, investigation, or prosecution of serious crime, including terrorism" and must use a specific identifier (i.e., name, account, or personal device);
- must be based on articulable and credible facts, particularity, legality, and severity of the conduct under investigation; and
- if the order is for the interception of wire or electronic communications, it must be of fixed, limited duration and can only be issued where that same information could not be reasonable obtained by a less intrusive method.

The executive agreement places further procedural requirements on the foreign government. The foreign government must:

- promptly review all material collected, and segregate, seal or delete (may not disseminate) material not found to be relevant to the request;
- not disseminate content of a US person to a US authority unless it relates to significant harm or threat of the US or US persons including crimes of national security, terrorism,
- violent crime, child exploitation, or significant financial fraud;
- afford reciprocal rights of data access to the US;
- agree to periodic reviews of compliance, with the US government reserving the right to rescind the agreement; and,
- the company would not be compelled under US law to respond to the request (but companies may, in reality, face other, non-legal pressures to comply).

The proposed legislation would also contain an "anti-cat's paw" provision, stating that the US cannot use this agreement to ask a foreign government to share information the US would not be able to obtain on its own[278]. This provision protects the privacy of US persons by requiring US government agencies to work through US channels to obtain data, rather than skirting legal requirements by turning to foreign partners with less restrictive practices to obtain the same data.
For instance, this provision prohibits US agencies from asking a foreign country to collect information about a US person through a request to a company, instead requiring US agencies to go through the established US warrant process to obtain that information.

These new bilateral agreements would augment, not replace, the current MLAT system. Foreign governments could still use the MLAT process for requests that fall outside the parameters of the executive agreement, or if they lack an executive agreement but have an MLAT.

Stated benefits

The proposal provides foreign countries the ability to make requests based on the law of the requesting country rather than US law, and allowing companies the option to respond without

[278] *Ibid*., §§ 4(a)(1)(xii), (xiii).

penalty under US law. This is likely to be welcomed by both companies and foreign public authorities. The proposal contains necessary limitations on this new process, including restricting requests under this agreement to serious crimes, placing limits on the ability to use this process to obtain information about US persons, requiring a degree of independent oversight of the requests, and prohibiting interception requests with open-ended timelines. Foreign governments would have the option to request both stored and real-time data. For responding companies, the proposed legislation does not compel response, it merely removes the legal barriers for responding, still giving companies a high degree of flexibility. In summary, the proposal creates a system with the potential to relieve the burdens on both foreign public authorities and US companies.

Stated concerns

Several civil society groups have voiced concerns about the draft proposal. A coalition of 21 organisations, including the Electronic Frontier Foundation, the Center for Democracy & Technology, Amnesty International and Human Rights Watch, sent a letter[279] to the US Congress in September 2017 opposing the bill[280].

The concerns are related to missing protections (some protections have been left out of the proposal) and reduced standards (the safeguards included in the proposal are not strict enough):

- Missing protections include:
  - The bill does not provide specific protections for **metadata**, which concerns actors who consider metadata just as useful to law enforcement and as privacy-invasive as content. Some argue that a court order should be required for the most-sensitive metadata[281]. It also remains to be seen how much companies will be able to push back on bad requests and what procedures of recourse would look like.
  - The bill does not mention **encryption** and whether providers could be subject to compelled assistance that goes beyond US law when dealing with foreign requests. As pro-encryption advocates point out, this bill also does not currently predicate access to data stored by US companies on the requesting country's pro-encryption

279 Access Now, Advocacy for Principled Action in Government, the American-Arab Anti-Discrimination Committee, the American Civil Liberties Union, Amnesty International, the Center for Democracy and Technology, the Center for Media and Democracy, the Constitutional Alliance, the Council on American-Islamic Relations, Defending Rights & Dissent, Demand Progress, Electronic Frontier Foundation, Fight for the Future, the Government Accountability Project, Government Information Watch, Human Rights Watch, the National Association of Criminal Defense Lawyers, National Security Counselors, New America's Open Technology Institute, the Project on Government Oversight, and Restore the Fourth, Coalition letter against DOJ's XBD bill, 9 September 2017.

280 For more information on the arguments of the letter, see Adam Schwartz and Lee Tien, Protect the Privacy of Cross-Border Data: Stop the DOJ Bill, EFF, 24 September 2017.

281 See Chris Calabrese, Statement to the U.S. House Committee on the Judiciary, Hearing on Data Stored Abroad:Ensuring Lawful Access and Privacy Protection in the Digital Era, June 15, 2017.

policy, such as prohibiting partner countries from passing anti-encryption legislation[282].

- The bill does not require **dual criminality**. In contrast, the current MLAT process requires dual criminality: a foreign government can only submit a request for data relating to a crime that is illegal both in their country and in the US Some advocates argue that the dual criminality piece is a critical feature, as it creates higher standards for civil liberties globally. Others, argue other countries should not be forced to follow standards that are not their own (provided they have met the requirements of the bilateral treaty).
- The bill lacks structured, explicit oversight over the request and response process. There is no requirement of **prior individualised review** and no standard mechanism for companies to challenge requests is included in the draft bill. This lack concerns civil society actors are concerned that requests and responses may push the boundaries of acceptability, given they are not individually subject to scrutiny.
- When striking agreements with other countries, the bill gives the ability to grant agreements solely with the **executive branch**, unlike the MLAT system, which requires Senate approval for each MLAT, increasing the risk of politicizing the approval process.
- There is **no requirement of notice**. The bill does not require any notice to the target of surveillance that foreign police seized their data.

- Reduced standards include:
  - Regarding evidentiary standards, the bill substitutes the current "**probable cause**" standard that applies to US MLATs with "reasonable justification based on articulable and credible facts[283]." Some argue that this change could mark a "dramatic elimination of a key civil liberties protection in US law[284]," as foreign states would no longer be required to meet the high US evidentiary standards to request data.
  - The bill does not enumerate specific requirements for qualifying for an executive agreement, but rather "factors" or "conditions" to be considered (e.g., meeting international human rights obligations, respect for rule of law). Civil society would prefer defined requirements that restrict the US government's ability to grant agreements based on politics.
  - The bill allows foreign governments to submit requests for **real-time surveillance**, a change from the current MLAT system, which focuses on stored communications.

---

282 See Jennifer Daskal. Statement to the Committee on the Judiciary Subcommittee on Crime and Terrorism United States Senate. Hearing on Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights, May 24, 2017.

283 U.S. Department of Justice, Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism, July 15, 2016, § 4(a)(3)(vii).

284 Center for Democracy & Technology, Cross-Border Law Enforcement Demands: Analysis of the US Department of Justice's Proposed Bill, Aug. 17, 2016.

Academics who have worked on the bill, including Jennifer Daskal and Andrew Woods, have also recognised many of these concerns, but they call for revision and iteration, not rejection, of the draft proposal[285].

[285] Jennifer Daskal and Andrew K. Woods, "Congress Should Embrace the DOJ's Cross-Border Data Fix," Just Security, August 1, 2016.

## ANNEX 11: ADDITIONAL DATA ON THE SIZE OF THE PROBLEM

Data from the survey of public authorities on cross-border access to e-evidence

The following tables and figures summarise the **results of the survey of public authorities** on cross-border access to e-evidence.[286] The survey comprised four main parts combining cooperation channel and location of the counterpart criterions. The requested data were broken down into eight respective categories based on its nature and type of the service provider, i.e. electronic communication services, telecommunication services, and internet or app-based services. The final results of the survey are divided into four categories – (1) relevance of cross-border access to e-evidence, (2) the request satisfaction rate, (3) percentage of investigations negatively affected, and (4) the time it takes to prepare a request and receive an answer.

*Relevance*

The targeted survey revealed that the electronic evidence in any form is **relevant** in 85% of investigations. [287] In approximately 65% of total investigations, the law enforcement authorities would need to make a request to a service provider in another jurisdiction to obtain the evidence.[288] The table 1 displays distribution of data requests among cooperation channels based on the nature of requested data and types of service providers criterions. However, the volume of cross-border requests for data the law enforcement authorities finally submit is lower than the number of cases where authorities would actually need to access the e-evidence.

*Table 1: the percentage of investigations where data request is submitted through different channels*

| | | | Within the EU | | With non-EU countries | |
|---|---|---|---|---|---|---|
| | | | **Judicial cooperation** | **Direct cooperation** | **Judicial cooperation** | **Direct cooperation** |
| **Non-content data** | **Subscriber data** | **Elect. comm.** | 25% | 15% | 25% | 25% |
| | | **Telco.** | 25% | 5% | 15% | 5% |
| | | **Inter/app.** | 15% | 5% | 15% | 5% |
| | **Metadata** | **Elect. comm.** | 25% | 5% | 15% | 5% |
| | | **Telco.** | 20% | 5% | 15% | 5% |
| | | **Inter/app.** | 15% | 5% | 15% | 5% |
| **Content data** | | **Elect. comm.** | 15% | 5% | 15% | 5% |
| | | **Inter/app.** | 15% | 5% | 15% | 5% |

[286] Targeted survey 2, Annex 2.1.
[287] Targeted survey feedback: Median of the respondents' estimations, 4 could not estimate (n=76).
[288] Targeted survey feedback: Median of the respondents' estimations, 6 could not estimate (n=76).

*Requests fulfilled*

The following table 2 indicates in detail the percentage of investigations where the request to service providers via the four different channels is **fulfilled**. The median of fulfilled request using both judicial and direct cooperation is 45%, according to the targeted survey respondents' estimations.

*Table 2: the percentage of investigations where the data request is fulfilled*

| | | | Within the EU | | With non-EU countries | |
|---|---|---|---|---|---|---|
| | | | **Judicial cooperation** | **Direct cooperation** | **Judicial cooperation** | **Direct cooperation** |
| **Non-content data** | **Subscriber data** | **Elect. comm.** | 75% | 55% | 45% | 55% |
| | | **Telco.** | 75% | 55% | 45% | 40% |
| | | **Inter/app.** | 65% | 65% | 45% | 45% |
| | **Metadata** | **Elect. comm.** | 65% | 45% | 30% | 35% |
| | | **Telco.** | 60% | 45% | 35% | 35% |
| | | **Inter/app.** | 55% | 55% | 35% | 35% |
| **Content data** | | **Elect. comm.** | 55% | 55% | 40% | 25% |
| | | **Inter/app.** | 55% | 55% | 45% | 35% |

The respondents further mentioned in their comments that it is common practice to send requests only to countries where authorities have already proved to be cooperative while some are not being contacted anymore based on a previous experience. Several most common causes for the e-evidence requests denials have been identified in the survey. Timely bureaucratic procedures and different legal standards are the most common obstacles when using judicial cooperation channels within the EU, yet it remains more effective compared to cooperation with non-EU counties. The respondents also mentioned the inability to identify a real geographic location of the providers, other legislative impediments, data availability and its accuracy in their comments.

*Investigations negatively affected*

The table 3 below demonstrates the percentage of investigations involving cross-border requests to access e-evidence that are **negatively affected** or cannot be pursued and its main cause.

*Table 3: the percentage of investigations involving requests to access to e-evidence across borders that are negatively affected or cannot be pursued*

| **Cause** | **Within the EU** | | **With non-EU countries** | |
|---|---|---|---|---|
| | **Judicial cooperation** | **Direct cooperation** | **Judicial cooperation** | **Direct cooperation** |
| Lack of timely access | 35% | 25% | 45% | 15% |
| Lack of access (access denied) | 25% | 25% | 25% | 15% |
| Other | 15% | 5% | 15% | 10% |
| **Total** | **75%** | **55%** | **85%** | **40%** |

*Time it takes*

The timely access to e-evidence matters as approximately one third of investigations concerning cross-border access to e-evidence are negatively affected or cannot be pursued precisely because of lack of timely access to the evidence (data not provided in time, e.g. leading to the disappearance of other leads), according to the law enforcement survey respondents. The time features for preparing and receiving a response through judicial cooperation channels or directly from a service provider reflect the other aspects of cross-border access to e-evidence as described earlier. The law enforcement authorities are regularly able to prepare and send a request within hours, eventually days; however, it usually takes several days, and can take up to months, to receive a response.

The **average time it takes** to prepare a cross-border request for data and receive an answer is displayed in the following figures. The respondents were asked to indicate the average time based on the previously used criterions of cooperation channels, types of the service provider and nature of the requested data.

- The figures 1, 2, 3, and 4 show the average time it takes to prepare **a request for content data** to all types of service providers located in the EU and in non-EU countries through different channels.
- The time it takes to prepare **a request for non-content data** is shown in the figures 5, 6, 7, and 8.
- The figures 9, 10, 11, and 12 show the average time it takes to receive **a response to a request for content data** to all types of service providers located in the EU and in non-EU countries through different channels.
- Finally, the figures 13, 14, 15, and 16 show the average time it takes to receive **a response to non-content data requests**.

*Figure 1: the time it takes to prepare a request for content data to service providers via public authorities in the EU*

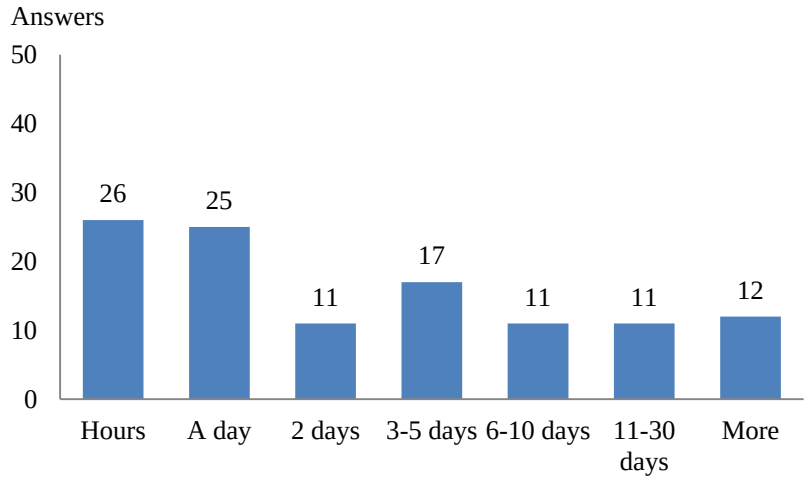



*Figure 2: the time it takes to prepare a direct request for content data to service providers in the EU*

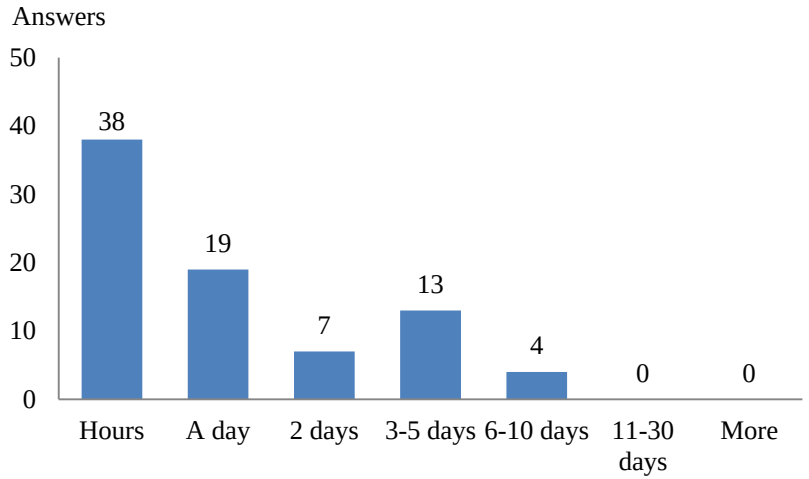



*Figure 3: the time it takes to prepare a request for content data to service providers via public authorities in non-EU countries*

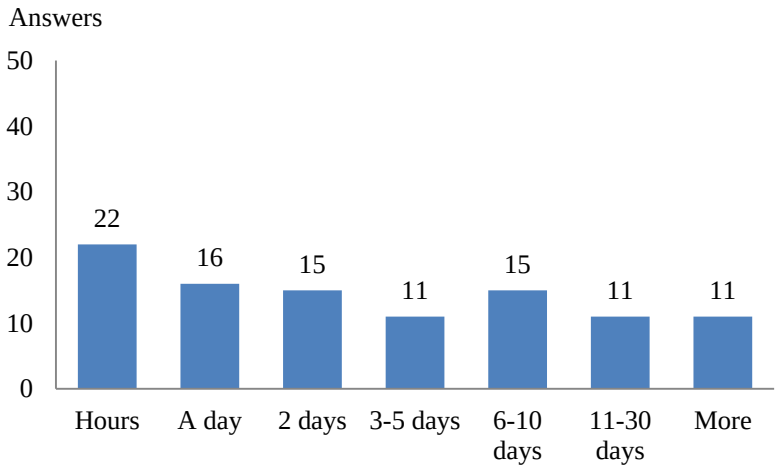



*Figure 4: the time it takes to prepare a direct request for content data to service providers in in non-EU countries*

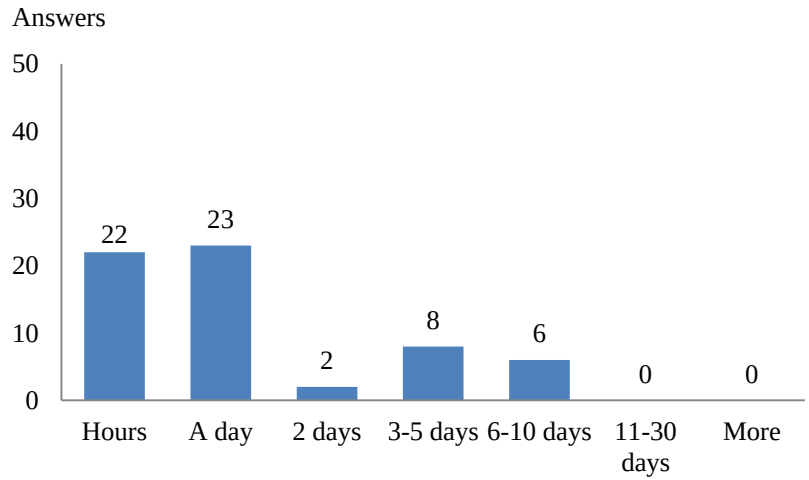


*Figure 5: the time it takes to prepare a request for non-content data to service providers via public authorities in the EU*

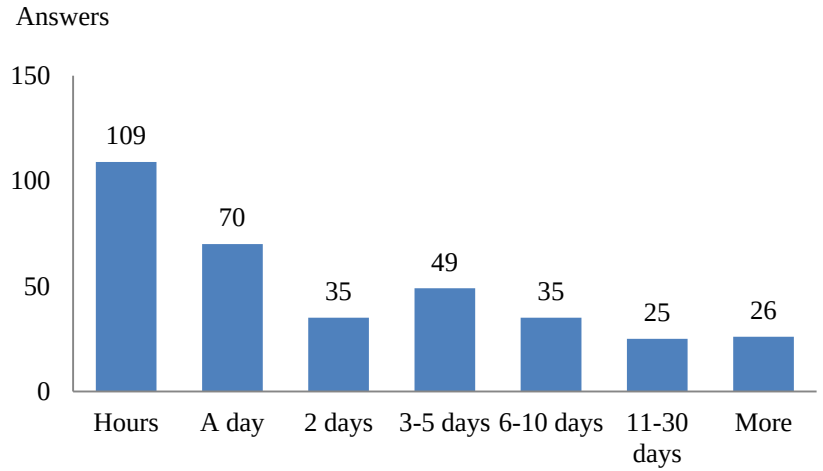



*Figure 6: the time it takes to prepare a direct request for non-content data to service providers in the EU*

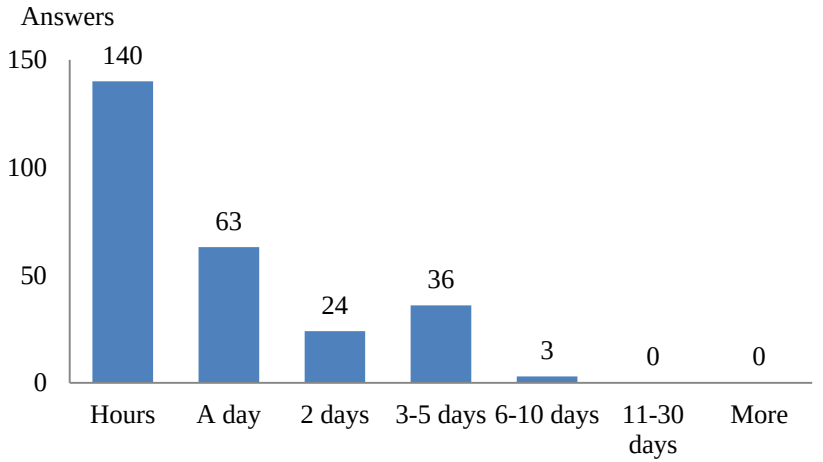



*Figure 7: the time it takes to prepare a request for non-content data to service providers via public authorities in non-EU countries*

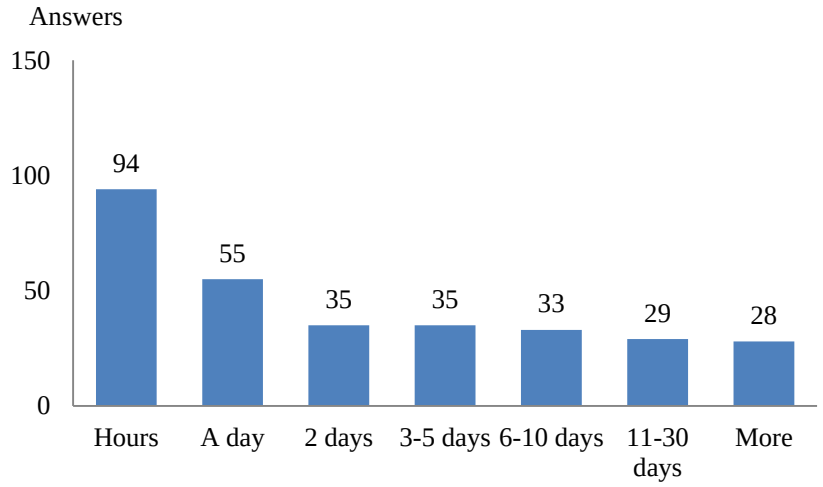



*Figure 8: the time it takes to prepare a direct request for non-content data to service providers in in non-EU countries*

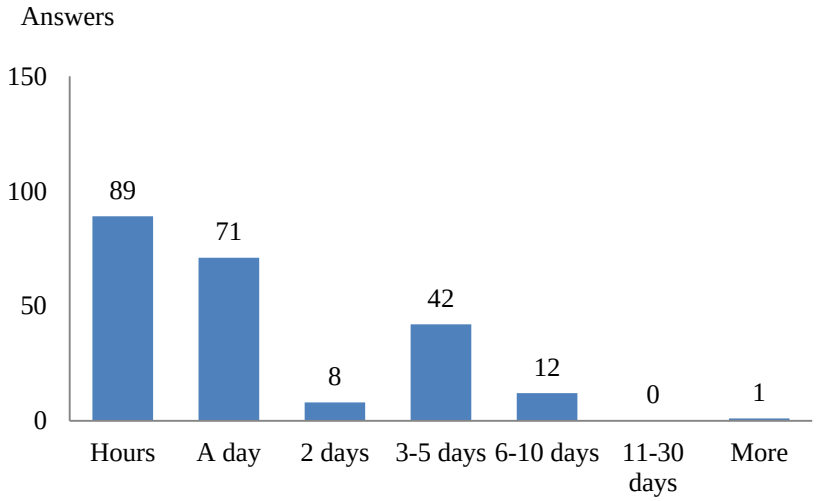


*Figure 9: the time it takes to receive a response to a request for content data to service providers via public authorities in the EU*

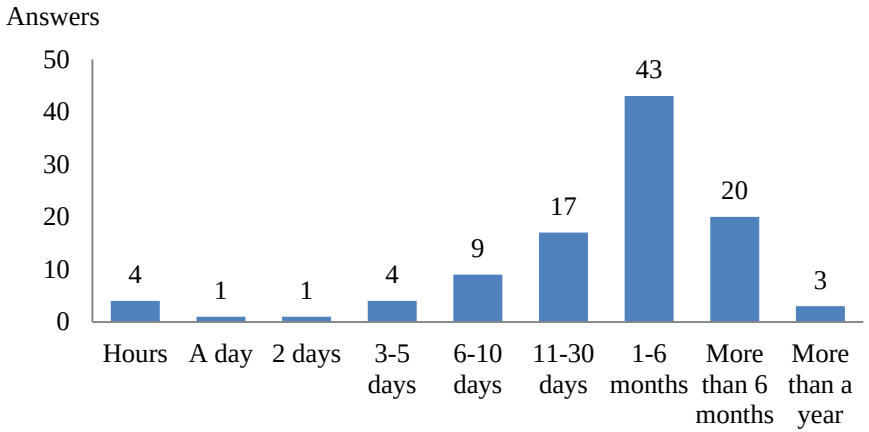



*Figure 10: the time it takes to receive a response to a direct request for content data to service providers in the EU*

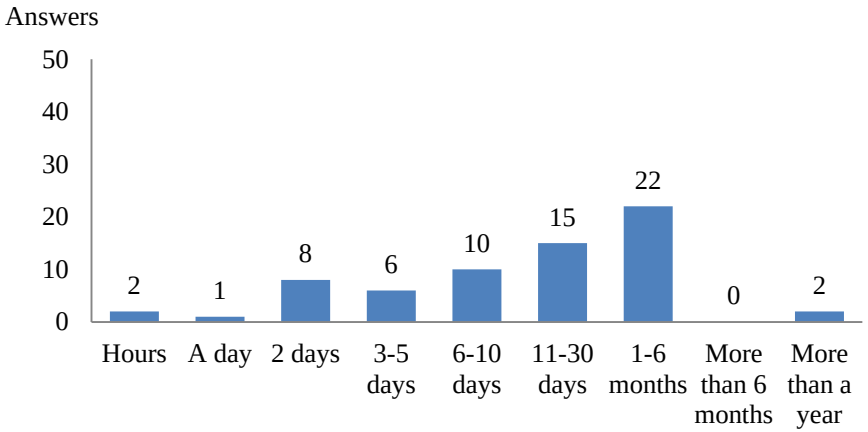



*Figure 11: the time it takes to receive a response to a request for content data to service providers via public authorities in non-EU countries*

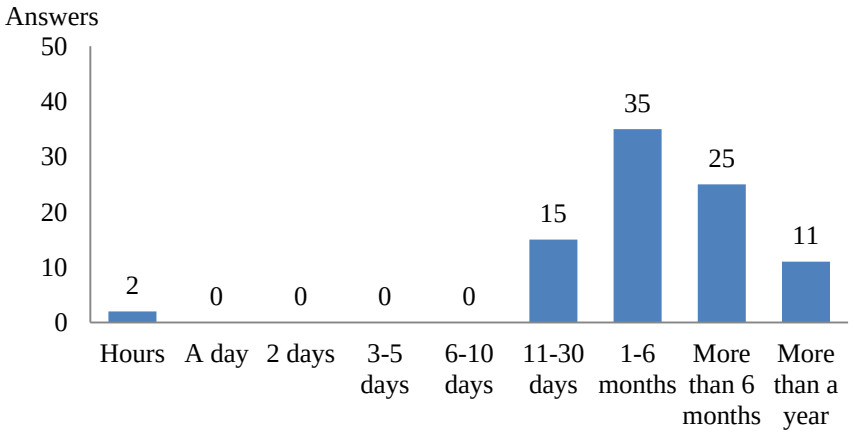



*Figure 12: the time it takes to receive a response to a direct content data request to service providers in non-EU countries*

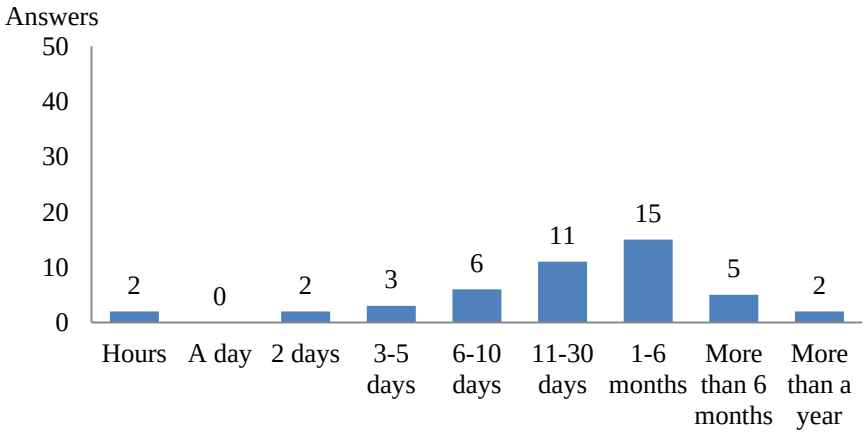


*Figure 13: the time it takes to receive a response to a request for non-content data to service providers via public authorities in the EU*

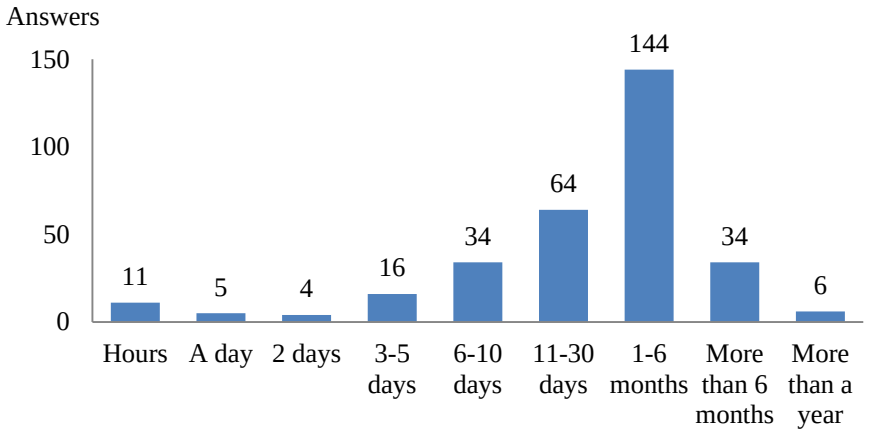



*Figure 14: the time it takes to receive a response to a direct request for non-content data to service providers in the EU*

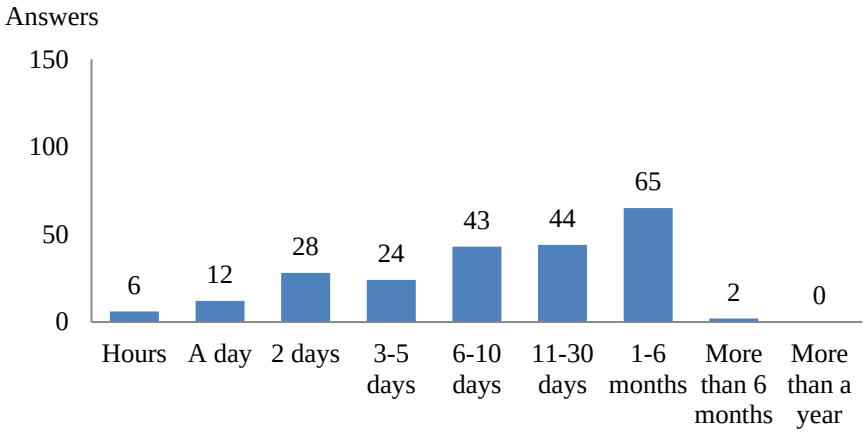



*Figure 15: the time it takes to receive a response to a request for non-content data to service providers via public authorities in non-EU countries*

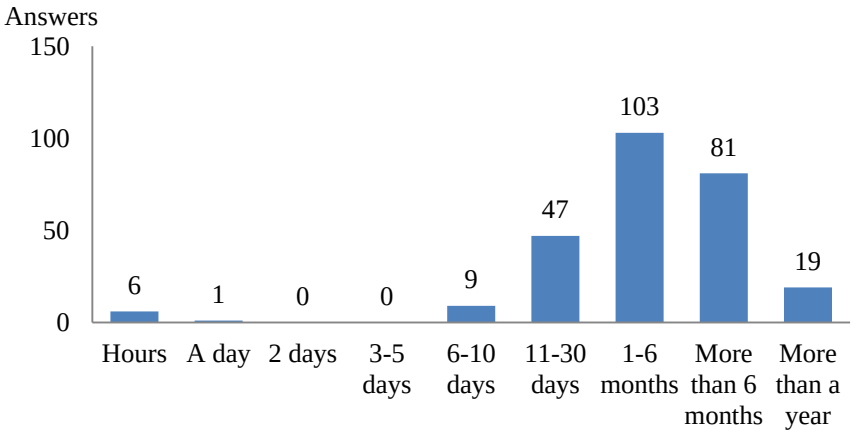
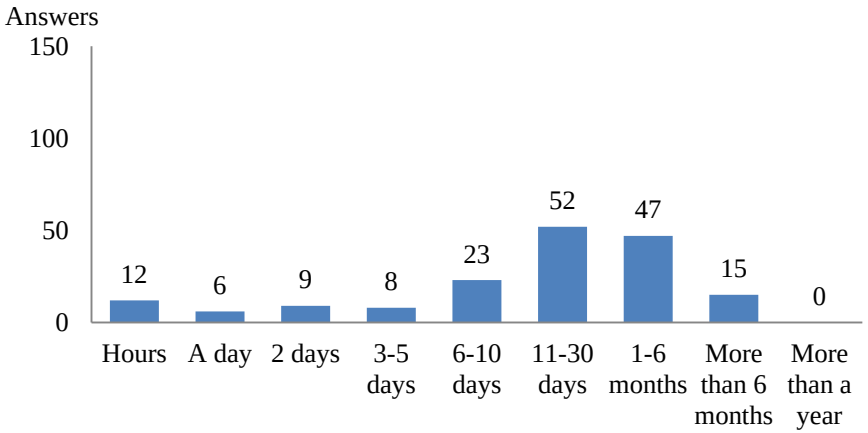



*Figure 16: the time it takes to receive a response to a direct non-content data request to service providers in non-EU countries*

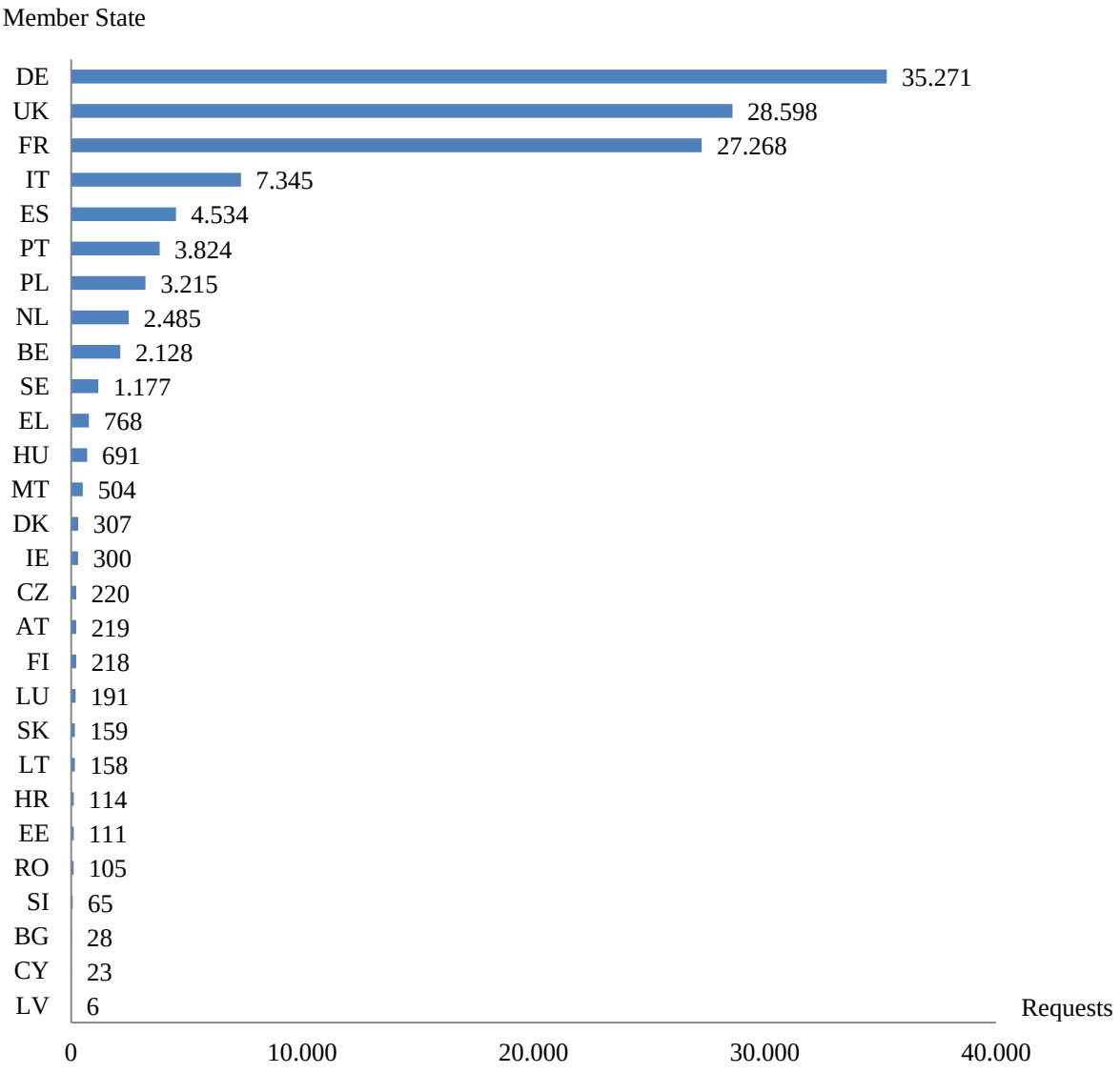


Data from transparency reports of selected service providers

As indicated in section 2.1.1.:

- Three Member States, **Germany, the UK and France**, accounted for **more than 75%** of the total number of requests to the main service providers in the last year:

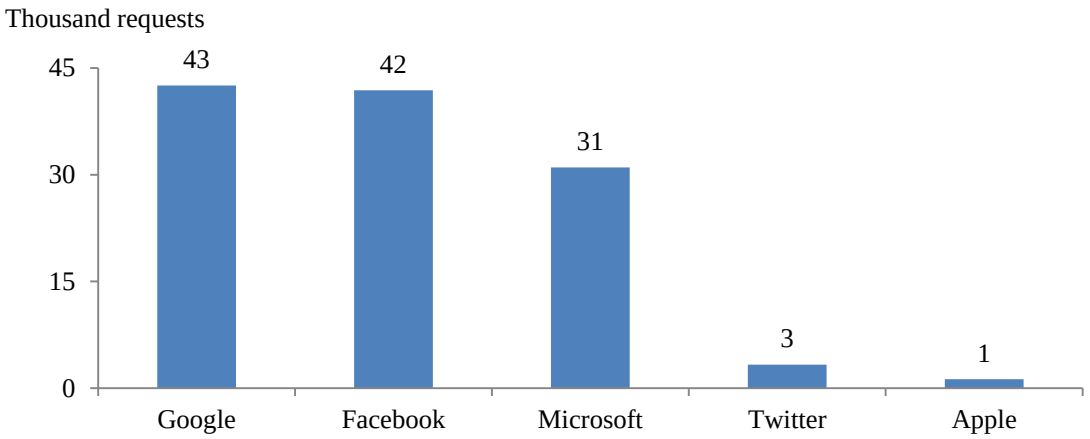
*Figure 17: number of requests[289] by Member State[290] (2016)*




- **Google and Facebook** accumulated **more than 70%** of the total number of requests from Member States to the main service providers in the last year:

[289] Requests to the five main service providers listed above.
[290] The list of country codes for Member States used in this document is available here.

*Figure 18: number of requests by service provider (2016)*




The following tables demonstrate the **volume of requests** for data to selected internet service providers by the current EU 28 Member States during the period from 2013 to 2016. The data were extracted from the respective providers' transparency registers available online[291]. The requests to providers are usually divided into subcategories depending on the provider – (a) emergency disclosure requests, (b) legal requests and (c) preservation requests. Apple also reports on device-based requests which are associated with devices or device connections to Apple services and requests for information regarding financial identifier; these figures comprise only account-based requests which are usually seeking details of customers using Apple's services such as iTunes or iCloud. Furthermore, some transparency reposts break down the statistics based on content or non-content data request criterion.

The presented figures consider primarily the **emergency and legal requests** for data submitted by law enforcement or judicial authorities of the Member States. The respective transparency reports are not always fully coherent, hence minor discrepancies which might have occurred in the presented figures should be taken into consideration. The transparency reports of Google and Apple do not differentiate between preservation requests and standard and emergency requests until 30 June 2014 and 31 December 2014 respectively. The presented figures therefore include all requests categories for Google and Apple until these dates and exclude emergency requests to Apple from 1 January 2015 onwards. The ratio between emergency and legal requests can vary depending on the country, e.g. Twitter reports that *17% of total global information requests received between January 1 and June 30, 2017 were emergency disclosure requests*; however, it is not indicated in the presented tables.

Table 4 presents the total volume of data requests submitted to the selected service providers by law enforcement authorities in Member States within the past four years and reveals its **continuous increase**. A single request can refer to multiple accounts, hence the accounts referenced and the number of data request is not a 1:1 ratio. Optionally, the same account may be the subject of several different requests. Moreover, the percentage of fulfilled requests does

[291] Google, Facebook, Microsoft, Twitter, Apple.

not necessary represent fully satisfied data requests from law enforcement and judicial authorities as the providers generally report on cases when some data were produced. The actual satisfaction rate may therefore be lower. The total volume of submitted data requests is then split in categories by the respective service providers in table 5 bellow.

*Table 4: data requests submitted, accounts referenced and percentage of requests where some date were produced (fulfilled requests)*

| | 1H 2013 | 2H 2013 | 1H 2014 | 2H 2014 | 1H 2015 | 2H 2015 | 1H 2016 | 2H 2016 |
|---|---|---|---|---|---|---|---|---|
| **Submitted requests** | 35295 | 36176 | 40194 | 39120 | 46762 | 54214 | 59858 | 60174 |
| **Accounts referenced** | 52408 | 54532 | 58639 | 57278 | 74503 | 92349 | 86417 | 84644 |
| **Fulfilled requests** | 45.65% | 44.82% | 44.87% | 43.57% | 44.49% | 47.70% | 53.00% | 58.15% |

*Table 5: data requests submitted to selected providers*

| | 1H 2013 | 2H 2013 | 1H 2014 | 2H 2014 | 1H 2015 | 2H 2015 | 1H 2016 | 2H 2016 |
|---|---|---|---|---|---|---|---|---|
| **Google** | 8299 | 9552 | 11201 | 11311 | 14278 | 18699 | 20675 | 21881 |
| **Facebook** | 8589 | 8368 | 10929 | 10575 | 13078 | 14757 | 19695 | 22191 |
| **Microsoft** | 17738 | 17531 | 17408 | 16625 | 18328 | 18832 | 17190 | 13835 |
| **Twitter** | 97 | 168 | 207 | 276 | 664 | 1413 | 1599 | 1707 |
| **Apple** | 572 | 557 | 449 | 333 | 414 | 513 | 699 | 560 |

The following table 6 displays the distribution of the volume of submitted data requests amongst respective Member States. Three Member States, **Germany, the UK and France**, representing slightly over 40% of the EU population, account for three quarters of the total number of requests to the main service providers submitted by law enforcement authorities in the EU.

*Table 6: data requests submitted by Member States*

| | 1H 2013 | 2H 2013 | 1H 2014 | 2H 2014 | 1H 2015 | 2H 2015 | 1H 2016 | 2H 2016 |
|---|---|---|---|---|---|---|---|---|
| **Austria** | 118 | 72 | 146 | 95 | 145 | 158 | 106 | 113 |
| **Belgium** | 857 | 701 | 859 | 940 | 936 | 1056 | 1088 | 1040 |
| **Bulgaria** | 3 | 6 | 5 | 0 | 6 | 2 | 12 | 16 |
| **Croatia** | 2 | 12 | 21 | 24 | 20 | 13 | 47 | 67 |
| **Cyprus** | 3 | 3 | 15 | 23 | 13 | 11 | 11 | 12 |
| **Czechia** | 46 | 63 | 52 | 65 | 90 | 89 | 105 | 115 |
| **Denmark** | 166 | 147 | 144 | 213 | 174 | 165 | 165 | 142 |
| **Estonia** | 3 | 21 | 20 | 15 | 27 | 52 | 59 | 52 |
| **Finland** | 41 | 73 | 78 | 65 | 74 | 153 | 125 | 93 |
| **France** | 8026 | 9214 | 9579 | 9816 | 10587 | 13932 | 13755 | 13513 |
| **Germany** | 9481 | 9701 | 11194 | 9539 | 10760 | 14856 | 16964 | 18307 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Greece** | 140 | 145 | 170 | 160 | 241 | 234 | 388 | 380 |
| **Hungary** | 181 | 136 | 132 | 206 | 306 | 275 | 401 | 290 |
| **Ireland** | 80 | 116 | 112 | 69 | 86 | 117 | 149 | 151 |
| **Italy** | 3540 | 3587 | 4019 | 3467 | 3857 | 3060 | 3771 | 3574 |
| **Latvia** | 1 | 1 | 2 | 0 | 0 | 0 | 3 | 3 |
| **Lithuania** | 12 | 26 | 25 | 23 | 71 | 87 | 82 | 76 |
| **Luxembourg** | 55 | 58 | 89 | 64 | 71 | 50 | 118 | 73 |
| **Malta** | 118 | 156 | 167 | 201 | 331 | 270 | 249 | 255 |
| **Netherlands** | 474 | 429 | 477 | 606 | 693 | 902 | 1121 | 1364 |
| **Poland** | 785 | 775 | 938 | 808 | 1196 | 1180 | 1588 | 1627 |
| **Portugal** | 774 | 804 | 1203 | 1002 | 1654 | 1585 | 2046 | 1778 |
| **Romania** | 16 | 27 | 36 | 43 | 51 | 25 | 43 | 62 |
| **Slovakia** | 15 | 50 | 46 | 58 | 60 | 42 | 70 | 89 |
| **Slovenia** | 6 | 6 | 5 | 5 | 6 | 15 | 35 | 30 |
| **Spain** | 2168 | 1768 | 2092 | 1941 | 2051 | 1809 | 2366 | 2168 |
| **Sweden** | 378 | 356 | 576 | 465 | 540 | 500 | 587 | 590 |
| **United Kingdom** | 7806 | 7723 | 7992 | 9207 | 12716 | 13576 | 14404 | 14194 |

The tables 7, 8, 9, 10, 11, 12, 13 and 14 present detailed information on the total volume of data requests to the selected providers, number of the accounts referenced and the rate of requests which have been fulfilled.

*Table 7: data requests submitted by Member States 1.7.2016 – 31.12.2016*

| | Facebook | | | Google | | | Microsoft | | | Twitter | | | Apple | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests |
| **Austria** | 47 | 55 | 40.43% | 44 | 64 | 21.50% | 18 | 41 | 83.33% | 1 | 1 | 100.00% | 3 | 4 | 33.00% |
| **Belgium** | 399 | 682 | 85.46% | 259 | 304 | 60.50% | 357 | 456 | 78.71% | 21 | 32 | 67.00% | 4 | 4 | 50.00% |
| **Bulgaria** | 14 | 20 | 64.29% | 2 | 3 | 0.00% | 0 | 0 | - | - | - | - | 0 | 0 | - |
| **Croatia** | 66 | 71 | 95.45% | 1 | 2 | 0.00% | 0 | 0 | - | - | - | - | 0 | 0 | - |
| **Cyprus** | 11 | 14 | 36.36% | 1 | 2 | 0 | 0 | 0 | - | - | - | - | 0 | 0 | - |
| **Czechia** | 61 | 82 | 77.05% | 0 | 0 | - | 50 | 297 | 76.00% | - | - | - | 4 | 4 | 100.00% |
| **Denmark** | 29 | 49 | 44.83% | 51 | 73 | 60.00% | 53 | 58 | 66.04% | 1 | 1 | 0.00% | 8 | 8 | 63.00% |
| **Estonia** | 17 | 20 | 82.35% | 32 | 58 | 34.00% | 0 | 0 | - | 1 | 1 | 0.00% | 2 | 2 | 100.00% |
| **Finland** | 34 | 51 | 82.35% | 40 | 48 | 37.50% | 18 | 50 | 72.22% | - | - | - | 1 | 1 | 0 |
| **France** | 4478 | 5195 | 68.38% | 4775 | 5738 | 59.50% | 3716 | 4918 | 56.54% | 474 | 572 | 68.00% | 70 | 76 | 59.00% |
| **Germany** | 4422 | 5631 | 54.03% | 9925 | 13320 | 50.50% | 3546 | 6254 | 69.51% | 255 | 311 | 38.00% | 159 | 268 | 70.00% |
| **Greece** | 275 | 393 | 67.27% | 78 | 104 | 65.00% | 16 | 17 | 62.50% | 8 | 21 | 13.00% | 3 | 3 | 100.00% |
| **Hungary** | 172 | 216 | 53.49% | 59 | 72 | 0.00% | 56 | 89 | 51.79% | 0 | 0 | - | 3 | 3 | 100.00% |
| **Ireland** | 79 | 83 | 79.75% | 19 | 34 | 34.00% | 48 | 70 | 56.25% | 3 | 6 | 100.00% | 2 | 2 | 50.00% |
| **Italy** | 1876 | 3230 | 60.07% | 1034 | 1486 | 18.50% | 471 | 913 | 52.44% | 149 | 184 | 78.00% | 44 | 53 | 89.00% |
| **Latvia** | 0 | 0 | - | 2 | 3 | 0.00% | 1 | 2 | 0 | 0 | 0 | - | 0 | 0 | - |
| **Lithuania** | 39 | 224 | 84.62% | 35 | 70 | 21.50% | 2 | 2 | 100.00% | - | - | - | 0 | 0 | - |
| **Luxembourg** | 0 | 0 | - | 0 | 0 | - | 71 | 246 | 77.46% | - | - | - | 2 | 5 | 0.5 |
| **Malta** | 173 | 189 | 72.83% | 64 | 93 | 29.50% | 15 | 16 | 73.33% | - | - | - | 3 | 3 | 100.00% |
| **Netherlands** | 630 | 1204 | 93.02% | 231 | 251 | 72.00% | 481 | 663 | 78.38% | 16 | 51 | 44.00% | 6 | 8 | 100.00% |
| **Poland** | 1060 | 1209 | 49.25% | 499 | 834 | 47.50% | 61 | 99 | 50.82% | 2 | 2 | 0.00% | 5 | 5 | 80.00% |
| **Portugal** | 738 | 818 | 52.71% | 610 | 702 | 33.00% | 423 | 500 | 66.90% | 3 | 3 | 33.00% | 4 | 4 | 75.00% |
| **Romania** | 29 | 81 | 58.62% | 28 | 70 | 23.00% | 5 | 21 | 40.00% | 0 | 0 | - | 0 | 0 | - |
| **Slovakia** | 18 | 21 | 83.33% | 57 | 65 | 0.00% | 14 | 34 | 71.43% | 0 | 0 | - | 0 | 0 | - |
| **Slovenia** | 13 | 13 | 69.23% | 17 | 60 | 14.50% | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Spain** | 833 | 1363 | 55.46% | 729 | 966 | 69.50% | 434 | 619 | 67.51% | 152 | 301 | 57.00% | 20 | 24 | 55.00% |
| **Sweden** | 312 | 596 | 89.10% | 112 | 159 | 84.00% | 133 | 236 | 81.20% | 15 | 18 | 73.00% | 18 | 21 | 78.00% |
| **United Kingdom** | 6366 | 7952 | 88.69% | 3177 | 5414 | 76.00% | 3846 | 6545 | 73.19% | 606 | 819 | 79.00% | 199 | 220 | 77.00% |
| **EU total** | **22191** | **29462** | **68.79%** | **21881** | **29995** | **35.06%** | **13835** | **22146** | **65.46%** | **1707** | **2323** | **50.00%** | **560** | **718** | **71.45%** |

*Table 8: data requests submitted by Member States 1.1.2016 – 30.6.2016*

| | Facebook | | | Google | | | Microsoft | | | Twitter | | | Apple | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests |
| **Austria** | 29 | 36 | 37.93% | 41 | 55 | 71.50% | 30 | 48 | 50.00% | 1 | 1 | 0.00% | 5 | 6 | 40.00% |
| **Belgium** | 420 | 674 | 86.43% | 248 | 326 | 55.50% | 351 | 453 | 78.71% | 67 | 75 | 88.00% | 2 | 2 | 100.00% |
| **Bulgaria** | 6 | 10 | 50.00% | 5 | 6 | 0.00% | 1 | 1 | 0.00% | - | - | - | 0 | 0 | - |
| **Croatia** | 47 | 53 | 93.62% | 0 | 0 | - | 0 | 0 | - | - | - | - | 0 | 0 | - |
| **Cyprus** | 10 | 14 | 0.00% | 0 | 0 | - | 1 | 1 | 0.00% | - | - | - | 0 | 0 | - |
| **Czechia** | 55 | 86 | 78.18% | 0 | 0 | - | 47 | 154 | 76.00% | 1 | 2 | 0.00% | 2 | 2 | 50.00% |
| **Denmark** | 34 | 52 | 47.05% | 58 | 96 | 55.50% | 68 | 131 | 66.04% | 4 | 10 | 75.00% | 1 | 1 | 100.00% |
| **Estonia** | 24 | 38 | 62.50% | 29 | 35 | 29.50% | 2 | 2 | 0.00% | 1 | 1 | 0.00% | 3 | 3 | 100.00% |
| **Finland** | 38 | 44 | 78.95% | 42 | 66 | 37.00% | 42 | 302 | 72.22% | 1 | 1 | 100.00% | 2 | 2 | 50.00% |
| **France** | 3763 | 4045 | 59.77% | 4300 | 5185 | 48.00% | 5045 | 7068 | 56.54% | 572 | 687 | 76.00% | 75 | 117 | 47.00% |
| **Germany** | 3695 | 4599 | 47.52% | 8788 | 13425 | 55.50% | 4167 | 7307 | 69.51% | 111 | 165 | 58.00% | 203 | 244 | 52.00% |
| **Greece** | 326 | 398 | 72.08% | 47 | 58 | 50.00% | 8 | 10 | 62.50% | 6 | 7 | 33.00% | 1 | 1 | 100.00% |
| **Hungary** | 186 | 230 | 46.78% | 166 | 218 | 0.00% | 45 | 194 | 51.79% | 0 | 0 | - | 4 | 4 | 50.00% |
| **Ireland** | 89 | 81 | 65.17% | 19 | 62 | 8.00% | 32 | 61 | 51.04% | 4 | 4 | 75.00% | 5 | 5 | 60.00% |
| **Italy** | 1913 | 2877 | 56.40% | 1092 | 1469 | 35.50% | 663 | 1247 | 52.44% | 58 | 80 | 47.00% | 45 | 54 | 38.00% |
| **Latvia** | 0 | 0 | - | 2 | 2 | 25.00% | 1 | 1 | 0.00% | 0 | 0 | - | 0 | 0 | - |
| **Lithuania** | 40 | 74 | 80.00% | 32 | 56 | 50.50% | 9 | 29 | 100.00% | 1 | 1 | 0.00% | 0 | 0 | - |
| **Luxembourg** | 2 | 2 | 100.00% | 0 | 0 | - | 109 | 494 | 78.81% | - | - | - | 7 | 10 | 29.00% |
| **Malta** | 146 | 169 | 78.08% | 75 | 82 | 30.00% | 23 | 28 | 73.33% | 2 | 2 | 0.00% | 3 | 3 | 100.00% |
| **Netherlands** | 450 | 758 | 87.11% | 268 | 280 | 67.00% | 385 | 441 | 78.38% | 8 | 11 | 38.00% | 10 | 10 | 50.00% |
| **Poland** | 991 | 1032 | 44.61% | 497 | 891 | 41.50% | 91 | 249 | 50.82% | 4 | 8 | 0.00% | 5 | 7 | 20.00% |
| **Portugal** | 785 | 848 | 48.67% | 731 | 860 | 31.50% | 522 | 595 | 66.90% | 3 | 3 | 0.00% | 5 | 5 | 40.00% |
| **Romania** | 25 | 37 | 48.00% | 17 | 27 | 23.50% | 1 | 1 | 40.00% | 0 | 0 | - | 0 | 0 | - |
| **Slovakia** | 24 | 32 | 66.67% | 38 | 40 | 5.50% | 8 | 76 | 71.43% | 0 | 0 | - | 0 | 0 | - |
| **Slovenia** | 14 | 15 | 64.29% | 20 | 90 | 25.00% | 0 | 0 | - | 0 | 0 | - | 1 | 1 | 100.00% |
| **Spain** | 811 | 1194 | 52.28% | 776 | 1046 | 73.50% | 623 | 946 | 67.51% | 117 | 295 | 57.00% | 39 | 100 | 49.00% |
| **Sweden** | 303 | 441 | 88.44% | 82 | 109 | 78.50% | 185 | 257 | 81.20% | 7 | 9 | 57.00% | 10 | 11 | 80.00% |
| **United Kingdom** | 5469 | 7199 | 86.63% | 3302 | 5219 | 76.00% | 4731 | 8249 | 73.19% | 631 | 1071 | 76.00% | 271 | 310 | 67.00% |
| **EU total** | **19695** | **25038** | **63.97%** | **20675** | **29703** | **40.56%** | **17190** | **28345** | **56.48%** | **1599** | **2433** | **41.05%** | **699** | **898** | **62.95%** |

*Table 9: data requests submitted by Member States 1.7.2015 – 31.12.2015*

| | Facebook | | | Google | | | Microsoft | | | Twitter | | | Apple | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Total requests** | **Accounts referenced** | **Fulfilled requests** | **Total requests** | **Accounts referenced** | **Fulfilled requests** | **Total requests** | **Accounts referenced** | **Fulfilled requests** | **Total requests** | **Accounts referenced** | **Fulfilled requests** | **Total requests** | **Accounts referenced** | **Fulfilled requests** |
| **Austria** | 54 | 54 | 33.33% | 30 | 39 | 18.50% | 62 | 478 | 41.94% | - | - | - | 12 | 12 | 67.00% |
| **Belgium** | 290 | 375 | 77.24% | 268 | 350 | 61.50% | 481 | 852 | 74.64% | 11 | 11 | 82.00% | 6 | 8 | 50.00% |
| **Bulgaria** | 0 | 0 | - | 2 | 2 | 0.00% | 0 | 0 | - | - | - | - | 0 | 0 | - |
| **Croatia** | 11 | 13 | 90.91% | 0 | 0 | - | 1 | 1 | 0.00% | 1 | 1 | 0.00% | 0 | 0 | - |
| **Cyprus** | 10 | 12 | 10.00% | 0 | 0 | - | 0 | 0 | - | - | - | - | 1 | 1 | 0.00% |
| **Czechia** | 17 | 18 | 41.18% | 0 | 0 | - | 64 | 136 | 60.94% | 3 | 3 | 0.00% | 5 | 5 | 20.00% |
| **Denmark** | 17 | 40 | 41.18% | 57 | 89 | 65.00% | 86 | 113 | 52.33% | 1 | 2 | 0.00% | 4 | 4 | 25.00% |
| **Estonia** | 21 | 22 | 66.67% | 27 | 38 | 32.50% | 4 | 5 | 50.00% | 0 | 0 | - | 0 | 0 | - |
| **Finland** | 39 | 69 | 71.79% | 52 | 79 | 37.50% | 56 | 305 | 76.79% | 3 | 5 | 100.00% | 3 | 3 | 67.00% |
| **France** | 2711 | 2894 | 54.22% | 4174 | 5126 | 44.00% | 6280 | 8613 | 57.98% | 707 | 866 | 61.00% | 60 | 65 | 30.00% |
| **Germany** | 3140 | 3628 | 42.26% | 7491 | 11562 | 59.50% | 4026 | 6585 | 67.69% | 69 | 80 | 55.00% | 130 | 150 | 52.00% |
| **Greece** | 186 | 266 | 71.51% | 30 | 33 | 41.00% | 10 | 13 | 50.00% | 8 | 8 | 13.00% | 0 | 0 | - |
| **Hungary** | 178 | 224 | 42.13% | 53 | 67 | 0.00% | 44 | 67 | 56.82% | 0 | 0 | - | 0 | 0 | - |
| **Ireland** | 56 | 55 | 69.64% | 15 | 12114 | 21.50% | 36 | 42 | 61.11% | 2 | 14 | 0.00% | 8 | 8 | 63.00% |
| **Italy** | 1525 | 2598 | 52.52% | 897 | 1124 | 20.50% | 572 | 2135 | 54.03% | 40 | 82 | 55.00% | 26 | 31 | 27.00% |
| **Latvia** | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Lithuania** | 33 | 36 | 42.42% | 46 | 275 | 63.50% | 8 | 11 | 50.00% | - | - | - | 0 | 0 | - |
| **Luxembourg** | 2 | 2 | 50.00% | 1 | 1 | 50.00% | 44 | 165 | 68.18% | 1 | 2 | 100.00% | 2 | 2 | 50.00% |
| **Malta** | 151 | 168 | 72.19% | 80 | 85 | 35.50% | 37 | 44 | 59.46% | 1 | 1 | 0.00% | 1 | 1 | 0.00% |
| **Netherlands** | 158 | 190 | 79.11% | 210 | 216 | 34.50% | 509 | 593 | 78.59% | 12 | 14 | 58.00% | 13 | 13 | 38.00% |
| **Poland** | 611 | 627 | 40.75% | 488 | 578 | 54.50% | 81 | 157 | 51.85% | - | - | - | 0 | 0 | - |
| **Portugal** | 545 | 623 | 30.09% | 587 | 698 | 29.00% | 445 | 561 | 68.54% | 1 | 1 | 0.00% | 7 | 8 | 57.00% |
| **Romania** | 11 | 18 | 9.09% | 14 | 21 | 28.50% | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Slovakia** | 0 | 0 | - | 30 | 39 | 8.50% | 12 | 16 | 66.67% | 0 | 0 | - | 0 | 0 | - |
| **Slovenia** | 5 | 3 | 20.00% | 8 | 11 | 50.00% | 2 | 2 | 100.00% | 0 | 0 | - | 0 | 0 | - |
| **Spain** | 536 | 947 | 44.96% | 599 | 848 | 51.00% | 528 | 1006 | 68.56% | 125 | 287 | 50.00% | 21 | 21 | 48.00% |
| **Sweden** | 260 | 400 | 87.31% | 43 | 76 | 78.50% | 190 | 314 | 71.58% | 1 | 1 | 100.00% | 6 | 6 | 33.00% |
| **United Kingdom** | 4190 | 5478 | 82.15% | 3497 | 5405 | 82.50% | 5254 | 9579 | 73.66% | 427 | 956 | 76.00% | 208 | 248 | 58.00% |
| **EU total** | **14757** | **18760** | **52.91%** | **18699** | **38876** | **40.31%** | **18832** | **31793** | **60.89%** | **1413** | **2334** | **44.12%** | **513** | **586** | **40.29%** |

*Table 10: data requests submitted by Member States 1.1.2015 – 30.6.2015*

| | Facebook | | | Google | | | Microsoft | | | Twitter | | | Apple | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests |
| **Austria** | 58 | 67 | 36.21% | 33 | 40 | 10.50% | 47 | 127 | 51.06% | - | - | - | 7 | 7 | 57.00% |
| **Belgium** | 281 | 356 | 68.68% | 243 | 311 | 85.50% | 406 | 600 | 73.15% | 5 | 7 | 40.00% | 1 | 1 | 100.00% |
| **Bulgaria** | 2 | 2 | 100.00% | 3 | 3 | 0.00% | 0 | 0 | - | 1 | 1 | 0.00% | 0 | 0 | - |
| **Croatia** | 18 | 20 | 44.44% | 0 | 0 | - | 2 | 2 | 50.00% | 0 | 0 | - | 0 | 0 | - |
| **Cyprus** | 8 | 8 | 12.50% | 1 | 1 | 0.00% | 1 | 1 | 100.00% | 1 | 1 | 0.00% | 2 | 2 | 50.00% |
| **Czechia** | 34 | 41 | 73.53% | 0 | 0 | - | 56 | 119 | 78.57% | 0 | 0 | - | 0 | 0 | - |
| **Denmark** | 49 | 80 | 38.78% | 55 | 79 | 27.50% | 67 | 91 | 67.16% | - | - | - | 3 | 3 | 33.00% |
| **Estonia** | 14 | 19 | 57.14% | 11 | 14 | 45.50% | 2 | 4 | 50.00% | 0 | 0 | - | 0 | 0 | - |
| **Finland** | 16 | 22 | 81.25% | 27 | 50 | 35.00% | 31 | 45 | 83.87% | 0 | 0 | - | 0 | 0 | - |
| **France** | 2520 | 2847 | 42.50% | 3489 | 4160 | 56.50% | 4396 | 6403 | 64.83% | 139 | 238 | 40.00% | 43 | 51 | 49.00% |
| **Germany** | 2344 | 2716 | 35.66% | 3903 | 6457 | 57.00% | 4407 | 8152 | 72.68% | 28 | 34 | 36.00% | 78 | 91 | 42.00% |
| **Greece** | 162 | 179 | 66.05% | 39 | 59 | 58.50% | 24 | 33 | 54.17% | 11 | 15 | 0.00% | 5 | 5 | 80.00% |
| **Hungary** | 185 | 224 | 36.22% | 50 | 59 | 0.00% | 68 | 90 | 69.12% | 0 | 0 | - | 3 | 3 | 0.00% |
| **Ireland** | 20 | 18 | 60.00% | 14 | 130 | 8.50% | 47 | 53 | 68.09% | 1 | 2 | 0.00% | 4 | 4 | 0.00% |
| **Italy** | 1816 | 2994 | 48.62% | 958 | 1242 | 21.50% | 1011 | 1532 | 66.96% | 43 | 103 | 16.00% | 29 | 32 | 48.00% |
| **Latvia** | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Lithuania** | 34 | 114 | 50.00% | 32 | 46 | 29.50% | 5 | 8 | 100.00% | - | - | - | 0 | 0 | - |
| **Luxembourg** | 5 | 5 | 20.00% | 0 | 0 | - | 66 | 259 | 72.73% | 0 | 0 | - | 0 | 0 | - |
| **Malta** | 152 | 193 | 71.05% | 112 | 121 | 27.00% | 65 | 76 | 56.92% | 0 | 0 | - | 2 | 2 | 100.00% |
| **Netherlands** | 113 | 111 | 66.37% | 162 | 166 | 70.50% | 397 | 593 | 83.12% | 18 | 25 | 33.00% | 3 | 3 | 33.00% |
| **Poland** | 492 | 444 | 34.35% | 629 | 839 | 43.50% | 74 | 92 | 55.41% | 1 | 1 | 0.00% | 0 | 0 | - |
| **Portugal** | 488 | 486 | 36.07% | 550 | 618 | 27.00% | 611 | 736 | 75.78% | 3 | 3 | 0.00% | 2 | 3 | 100.00% |
| **Romania** | 25 | 70 | 28.00% | 25 | 55 | 28.00% | 0 | 0 | - | 0 | 0 | - | 1 | 1 | 0.00% |
| **Slovakia** | 0 | 0 | - | 47 | 56 | 11.50% | 13 | 14 | 38.46% | 0 | 0 | - | 0 | 0 | - |
| **Slovenia** | 1 | 2 | 0.00% | 3 | 4 | 33.50% | 2 | 2 | 50.00% | 0 | 0 | - | 0 | 0 | - |
| **Spain** | 619 | 1000 | 41.33% | 715 | 941 | 25.50% | 588 | 839 | 71.94% | 110 | 310 | 24.00% | 19 | 24 | 53.00% |
| **Sweden** | 238 | 348 | 87.82% | 31 | 50 | 34.50% | 262 | 584 | 78.24% | 4 | 4 | 50.00% | 5 | 5 | 20.00% |
| **United Kingdom** | 3384 | 4489 | 78.04% | 3146 | 6056 | 82.50% | 5680 | 13382 | 74.19% | 299 | 1041 | 52.00% | 207 | 232 | 63.00% |
| **EU total** | **13078** | **16855** | **50.56%** | **14278** | **21557** | **34.13%** | **18328** | **33837** | **68.26%** | **664** | **1785** | **20.79%** | **414** | **469** | **48.71%** |

*Table 11: data requests submitted by Member States 1.7.2014 – 31.12.2014*

| | Facebook | | | Google | | | Microsoft | | | Twitter | | | Apple | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests |
| **Austria** | 46 | 63 | 10.87% | 24 | 31 | 6.50% | 21 | 44 | 38.10% | - | - | - | 4 | 4 | 100.00% |
| **Belgium** | 239 | 319 | 59.00% | 214 | 297 | 67.00% | 481 | 765 | 81.91% | 1 | 1 | 0.00% | 5 | 5 | 20.00% |
| **Bulgaria** | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | - | - | - | 0 | 0 | - |
| **Croatia** | 21 | 28 | 80.95% | 2 | 3 | 0.00% | 1 | 4 | 100.00% | 0 | 0 | - | 0 | 0 | - |
| **Cyprus** | 20 | 26 | 60.00% | 0 | 0 | - | 3 | 3 | 0.00% | 0 | 0 | - | 0 | 0 | - |
| **Czechia** | 22 | 132 | 54.55% | 0 | 0 | - | 42 | 63 | 90.48% | 0 | 0 | - | 1 | 1 | 0.00% |
| **Denmark** | 31 | 33 | 35.48% | 67 | 78 | 27.50% | 106 | 186 | 79.25% | 3 | 3 | 33.00% | 6 | 6 | 50.00% |
| **Estonia** | 6 | 7 | 66.67% | 5 | 6 | 10.00% | 4 | 6 | 50.00% | 0 | 0 | - | 0 | 0 | - |
| **Finland** | 18 | 28 | 72.22% | 18 | 32 | 36.00% | 29 | 64 | 58.62% | 0 | 0 | - | 0 | 0 | - |
| **France** | 2094 | 2885 | 42.41% | 3073 | 3752 | 53.50% | 4546 | 6851 | 79.78% | 60 | 81 | 13.00% | 43 | 43 | 26.00% |
| **Germany** | 2132 | 2611 | 34.29% | 3114 | 3878 | 51.50% | 4192 | 7629 | 79.20% | 17 | 18 | 12.00% | 84 | 90 | 42.00% |
| **Greece** | 117 | 142 | 57.26% | 22 | 37 | 37.50% | 18 | 23 | 50.00% | 3 | 5 | 0.00% | 0 | 0 | - |
| **Hungary** | 128 | 167 | 34.38% | 21 | 27 | 0.00% | 57 | 79 | 82.46% | 0 | 0 | - | 0 | 0 | - |
| **Ireland** | 34 | 34 | 70.59% | 7 | 78 | 75.00% | 27 | 31 | 70.37% | - | - | - | 1 | 1 | 25.00% |
| **Italy** | 1774 | 2696 | 46.45% | 914 | 1130 | 42.50% | 759 | 957 | 67.59% | - | - | - | 20 | 20 | 40.00% |
| **Latvia** | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Lithuania** | 12 | 21 | 41.67% | 6 | 7 | 33.50% | 5 | 29 | 80.00% | - | - | - | 0 | 0 | - |
| **Luxembourg** | 1 | 4 | 100.00% | 0 | 0 | - | 54 | 129 | 74.07% | 0 | 0 | - | 9 | 9 | 44.00% |
| **Malta** | 93 | 112 | 70.97% | 57 | 61 | 25.50% | 50 | 52 | 84.00% | 0 | 0 | - | 1 | 1 | 100.00% |
| **Netherlands** | 76 | 84 | 64.47% | 140 | 144 | 40.50% | 381 | 478 | 81.36% | 4 | 8 | 25.00% | 5 | 5 | 40.00% |
| **Poland** | 305 | 349 | 29.84% | 455 | 584 | 35.50% | 47 | 62 | 74.47% | 0 | 0 | - | 1 | 1 | 0.00% |
| **Portugal** | 305 | 365 | 34.75% | 309 | 381 | 27.00% | 386 | 461 | 86.79% | 1 | 1 | 0.00% | 1 | 1 | 100.00% |
| **Romania** | 14 | 35 | 42.86% | 29 | 65 | 24.00% | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Slovakia** | 5 | 5 | 20.00% | 33 | 42 | 4.50% | 20 | 25 | 85.00% | 0 | 0 | - | 0 | 0 | - |
| **Slovenia** | 3 | 3 | 33.33% | 1 | 1 | 50.00% | 1 | 1 | 100.00% | 0 | 0 | - | 0 | 0 | - |
| **Spain** | 500 | 1041 | 37.00% | 698 | 961 | 76.50% | 655 | 1257 | 78.17% | 69 | 104 | 12.00% | 19 | 20 | 26.00% |
| **Sweden** | 213 | 289 | 76.06% | 22 | 25 | 20.50% | 222 | 340 | 86.04% | 2 | 2 | 0.00% | 6 | 8 | 33.00% |
| **United Kingdom** | 2366 | 2890 | 75.11% | 2080 | 2755 | 83.50% | 4518 | 8034 | 75.12% | 116 | 371 | 34.00% | 127 | 152 | 53.00% |
| **EU total** | **10575** | **14369** | **51.97%** | **11311** | **14375** | **36.00%** | **16625** | **27573** | **73.31%** | **276** | **594** | **12.90%** | **333** | **367** | **43.69%** |

*Table 12: data requests submitted by Member States 1.1.2014 – 30.6.2014*

| | Facebook | | | Google | | | Microsoft | | | Twitter | | | Apple | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests |
| **Austria** | 63 | 84 | 17.46% | 47 | 58 | 34.00% | 30 | 67 | 70.00% | - | - | - | 6 | 6 | 83.00% |
| **Belgium** | 209 | 246 | 56.94% | 213 | 513 | 73.00% | 433 | 922 | 83.14% | - | - | - | 4 | 4 | 50.00% |
| **Bulgaria** | 3 | 4 | 100.00% | 1 | 2 | 0.00% | 0 | 0 | - | - | - | - | 1 | 1 | 0.00% |
| **Croatia** | 19 | 24 | 78.95% | 1 | 1 | 0.00% | 1 | 1 | 100.00% | 0 | 0 | - | 0 | 0 | - |
| **Cyprus** | 13 | 16 | 69.23% | 0 | 0 | - | 2 | 2 | 0.00% | 0 | 0 | - | 0 | 0 | - |
| **Czechia** | 11 | 12 | 27.27% | 0 | 0 | - | 41 | 102 | 87.80% | 0 | 0 | - | - | - | - |
| **Denmark** | 15 | 17 | 40.00% | 52 | 68 | 50.00% | 72 | 122 | 80.56% | 1 | 1 | 0.00% | 4 | 4 | 0.00% |
| **Estonia** | 7 | 7 | 42.86% | 3 | 3 | 67.00% | 10 | 11 | 70.00% | 0 | 0 | - | 0 | 0 | - |
| **Finland** | 28 | 32 | 42.86% | 17 | 31 | 94.00% | 33 | 48 | 93.94% | 0 | 0 | - | - | - | - |
| **France** | 2249 | 2599 | 30.24% | 3002 | 3826 | 59.00% | 4220 | 6094 | 80.09% | 36 | 51 | 8.00% | 72 | 92 | 31.00% |
| **Germany** | 2537 | 3078 | 33.94% | 3338 | 4272 | 48.00% | 5183 | 8295 | 78.66% | 14 | 28 | 21.00% | 122 | 254 | 43.00% |
| **Greece** | 128 | 167 | 56.25% | 16 | 41 | 38.00% | 10 | 11 | 50.00% | 16 | 37 | 13.00% | 0 | 0 | - |
| **Hungary** | 57 | 78 | 33.33% | 17 | 23 | 0.00% | 58 | 83 | 84.48% | 0 | 0 | - | 0 | 0 | - |
| **Ireland** | 54 | 50 | 61.11% | 10 | 10 | 30.00% | 38 | 76 | 78.95% | 3 | 4 | 33.00% | 7 | 12 | 14.00% |
| **Italy** | 1869 | 2658 | 49.28% | 1108 | 1401 | 43.00% | 1010 | 1491 | 72.18% | 10 | 19 | 20.00% | 22 | 22 | 41.00% |
| **Latvia** | 0 | 0 | - | 0 | 0 | - | 2 | 5 | 100.00% | 0 | 0 | - | 0 | 0 | - |
| **Lithuania** | 8 | 9 | 37.50% | 6 | 7 | 83.00% | 10 | 45 | 60.00% | 1 | 1 | 0.00% | 0 | 0 | - |
| **Luxembourg** | 4 | 5 | 25.00% | 1 | 2 | 0.00% | 84 | 847 | 84.52% | 0 | 0 | - | - | - | - |
| **Malta** | 85 | 94 | 62.35% | 42 | 53 | 67.00% | 40 | 42 | 72.50% | 0 | 0 | - | 0 | 0 | - |
| **Netherlands** | 41 | 45 | 56.10% | 72 | 95 | 82.00% | 353 | 470 | 84.14% | 5 | 8 | 20.00% | 6 | 7 | 33.00% |
| **Poland** | 288 | 377 | 27.08% | 591 | 767 | 28.00% | 56 | 91 | 66.07% | 0 | 0 | - | 3 | 3 | 67.00% |
| **Portugal** | 354 | 403 | 40.40% | 338 | 398 | 53.00% | 511 | 610 | 83.17% | - | - | - | - | - | - |
| **Romania** | 16 | 20 | 50.00% | 20 | 56 | 60.00% | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Slovakia** | 0 | 0 | - | 29 | 50 | 7.00% | 17 | 17 | 76.47% | 0 | 0 | - | 0 | 0 | - |
| **Slovenia** | 0 | 0 | - | 4 | 4 | 50.00% | 1 | 1 | 100.00% | 0 | 0 | - | 0 | 0 | - |
| **Spain** | 514 | 860 | 36.58% | 696 | 921 | 46.00% | 829 | 1460 | 82.03% | 43 | 64 | 12.00% | 10 | 11 | 30.00% |
| **Sweden** | 247 | 334 | 80.57% | 42 | 94 | 31.00% | 274 | 547 | 84.31% | - | - | - | 13 | 23 | 38.00% |
| **United Kingdom** | 2110 | 2619 | 71.68% | 1535 | 1991 | 72.00% | 4090 | 7562 | 78.44% | 78 | 220 | 46.00% | 179 | 220 | 43.00% |
| **EU total** | **10929** | **13838** | **49.08%** | **11201** | **14687** | **44.60%** | **17408** | **29022** | **76.98%** | **207** | **433** | **17.30%** | **449** | **659** | **36.38%** |

*Table 13: data requests submitted by Member States 1.7.2013 – 31.12.2013*

| | Facebook | | | Google | | | Microsoft | | | Twitter | | | Apple | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests |
| **Austria** | 28 | 32 | 14.29% | 23 | 114 | 26.00% | 15 | 109 | 53.33% | - | - | - | 6 | 6 | 17.00% |
| **Belgium** | 154 | 196 | 64.94% | 162 | 206 | 73.00% | 378 | 520 | 75.93% | 2 | 2 | 50.00% | 5 | 5 | 20.00% |
| **Bulgaria** | 2 | 2 | 50.00% | 1 | 3 | 0.00% | 3 | 4 | 100.00% | - | - | - | - | - | - |
| **Croatia** | 7 | 14 | 42.86% | 3 | 6 | 0.00% | 2 | 2 | 100.00% | 0 | 0 | - | 0 | 0 | - |
| **Cyprus** | 3 | 3 | 100.00% | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Czechia** | 14 | 19 | 78.57% | 0 | 0 | - | 44 | 79 | 90.91% | 0 | 0 | - | 5 | 5 | 20.00% |
| **Denmark** | 12 | 11 | 33.33% | 58 | 65 | 62.00% | 70 | 83 | 75.71% | - | - | - | 7 | 7 | 57.00% |
| **Estonia** | 6 | 7 | 33.33% | 2 | 4 | 50.00% | 13 | 18 | 69.23% | 0 | 0 | - | 0 | 0 | - |
| **Finland** | 11 | 12 | 63.64% | 13 | 48 | 92.00% | 47 | 79 | 72.34% | 0 | 0 | - | 2 | 2 | 50.00% |
| **France** | 1661 | 1845 | 33.90% | 2750 | 3378 | 51.00% | 4627 | 6956 | 78.15% | 57 | 102 | 23.00% | 119 | 130 | 29.00% |
| **Germany** | 1687 | 1950 | 37.88% | 2660 | 3255 | 40.00% | 5204 | 8895 | 79.88% | 3 | 3 | 33.00% | 147 | 160 | 46.00% |
| **Greece** | 115 | 148 | 50.43% | 13 | 29 | 15.00% | 8 | 9 | 75.00% | 9 | 9 | 11.00% | 0 | 0 | - |
| **Hungary** | 38 | 51 | 28.95% | 42 | 42 | 0.00% | 56 | 68 | 83.93% | 0 | 0 | - | 0 | 0 | - |
| **Ireland** | 35 | 36 | 62.86% | 15 | 51 | 27.00% | 58 | 81 | 77.59% | - | - | - | 8 | 8 | 25.00% |
| **Italy** | 1699 | 2613 | 52.50% | 896 | 1084 | 42.00% | 933 | 1240 | 75.35% | 19 | 19 | 0.00% | 40 | 43 | 28.00% |
| **Latvia** | 0 | 0 | - | 0 | 0 | - | 1 | 1 | 0.00% | 0 | 0 | - | 0 | 0 | - |
| **Lithuania** | 9 | 10 | 44.44% | 11 | 18 | 64.00% | 6 | 11 | 66.67% | 0 | 0 | - | 0 | 0 | - |
| **Luxembourg** | 2 | 5 | 0.00% | 0 | 0 | - | 47 | 91 | 76.60% | 0 | 0 | - | 9 | 9 | 89.00% |
| **Malta** | 81 | 127 | 61.73% | 54 | 60 | 83.00% | 21 | 24 | 90.48% | 0 | 0 | - | 0 | 0 | - |
| **Netherlands** | 23 | 28 | 36.36% | 53 | 63 | 75.00% | 338 | 1551 | 71.60% | 9 | 14 | 56.00% | 6 | 7 | 0.00% |
| **Poland** | 220 | 192 | 15.45% | 502 | 740 | 23.00% | 52 | 100 | 84.62% | 0 | 0 | - | 1 | 1 | 0.00% |
| **Portugal** | 148 | 175 | 25.00% | 283 | 347 | 45.00% | 372 | 483 | 86.56% | - | - | - | 1 | 1 | 100.00% |
| **Romania** | 11 | 20 | 45.45% | 16 | 33 | 56.00% | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Slovakia** | 0 | 0 | - | 34 | 37 | 15.00% | 16 | 18 | 87.50% | 0 | 0 | - | 0 | 0 | - |
| **Slovenia** | 3 | 3 | 66.67% | 1 | 1 | 0.00% | 2 | 1 | 0.00% | 0 | 0 | - | 0 | 0 | - |
| **Spain** | 404 | 811 | 39.60% | 545 | 761 | 53.00% | 769 | 1238 | 79.58% | 13 | 26 | 0.00% | 37 | 41 | 35.00% |
| **Sweden** | 89 | 109 | 52.81% | 18 | 19 | 28.00% | 236 | 478 | 79.66% | - | - | - | 13 | 19 | 23.00% |
| **United Kingdom** | 1906 | 2277 | 71.30% | 1397 | 3142 | 69.00% | 4213 | 7276 | 78.73% | 56 | 117 | 43.00% | 151 | 179 | 38.00% |
| **EU total** | **8368** | **10696** | **46.40%** | **9552** | **13506** | **41.21%** | **17531** | **29415** | **73.44%** | **168** | **292** | **27.00%** | **557** | **623** | **36.06%** |

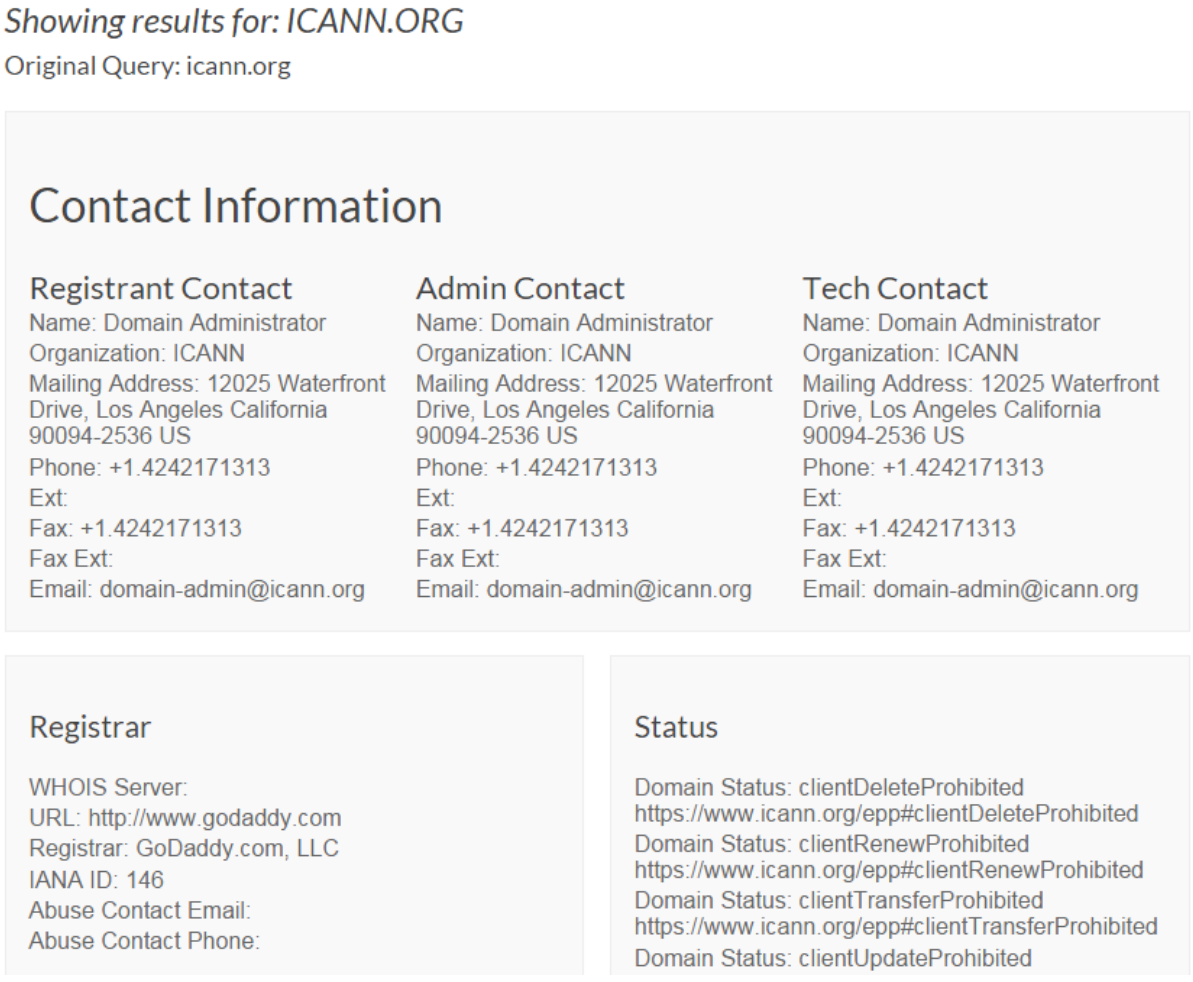
*Table 14: data requests submitted by Member States 1.1.2013 – 30.6.2013*

| | Facebook | | | Google | | | Microsoft | | | Twitter | | | Apple | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests | Total requests | Accounts referenced | Fulfilled requests |
| **Austria** | 35 | 41 | 17.00% | 0 | 0 | - | 9 | 15 | 77.78% | - | - | - | 74 | 2 | 50.00% |
| **Belgium** | 150 | 169 | 70.00% | 194 | 289 | 66.00% | 500 | 784 | 81.20% | - | - | - | 13 | 20 | 38.00% |
| **Bulgaria** | 1 | 1 | 0.00% | 0 | 0 | - | 2 | 4 | 100.00% | - | - | - | 0 | 0 | - |
| **Croatia** | 2 | 2 | 0.00% | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Cyprus** | 3 | 4 | 33.00% | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Czechia** | 10 | 13 | 60.00% | 0 | 0 | - | 34 | 62 | 76.47% | 0 | 0 | - | 2 | 2 | 50.00% |
| **Denmark** | 11 | 11 | 55.00% | 37 | 56 | 65.00% | 107 | 256 | 83.18% | - | - | - | 11 | 11 | 55.00% |
| **Estonia** | 0 | 0 | - | 0 | 0 | - | 3 | 6 | 100.00% | 0 | 0 | - | 0 | 0 | - |
| **Finland** | 12 | 15 | 75.00% | 0 | 0 | - | 29 | 48 | 86.21% | 0 | 0 | - | 0 | 0 | - |
| **France** | 1547 | 1598 | 39.00% | 2011 | 2481 | 49.00% | 4379 | 7926 | 82.19% | 18 | 35 | 11.00% | 71 | 72 | 24.00% |
| **Germany** | 1886 | 2068 | 37.00% | 2311 | 3079 | 48.00% | 5185 | 9670 | 83.28% | 6 | 6 | 17.00% | 93 | 93 | 6.00% |
| **Greece** | 122 | 141 | 54.00% | 0 | 0 | - | 10 | 64 | 90.00% | 8 | 9 | 0.00% | 0 | 0 | - |
| **Hungary** | 25 | 24 | 36.00% | 86 | 104 | 0.00% | 70 | 127 | 82.86% | 0 | 0 | - | 0 | 0 | - |
| **Ireland** | 34 | 40 | 71.00% | 0 | 0 | - | 40 | 69 | 50.00% | 1 | 1 | 100.00% | 5 | 5 | 60.00% |
| **Italy** | 1705 | 2306 | 53.00% | 901 | 1222 | 38.00% | 852 | 1172 | 78.17% | 22 | 22 | 0.00% | 60 | 76 | 37.00% |
| **Latvia** | 0 | 0 | - | 0 | 0 | - | 1 | 1 | 100.00% | 0 | 0 | - | 0 | 0 | - |
| **Lithuania** | 6 | 7 | 17.00% | 0 | 0 | - | 6 | 20 | 50.00% | 0 | 0 | - | 0 | 0 | - |
| **Luxembourg** | 0 | 0 | - | 0 | 0 | - | 55 | 121 | 78.18% | 0 | 0 | - | 0 | 0 | - |
| **Malta** | 89 | 97 | 60.00% | 0 | 0 | - | 29 | 34 | 82.76% | 0 | 0 | - | 0 | 0 | - |
| **Netherlands** | 11 | 15 | 36.00% | 45 | 46 | 64.00% | 411 | 714 | 78.10% | 3 | 3 | 33.00% | 4 | 4 | 25.00% |
| **Poland** | 233 | 158 | 9.00% | 496 | 597 | 23.00% | 55 | 76 | 72.73% | 0 | 0 | - | 1 | 2 | 0.00% |
| **Portugal** | 177 | 213 | 42.00% | 261 | 322 | 30.00% | 334 | 411 | 81.74% | - | - | - | 2 | 2 | 100.00% |
| **Romania** | 16 | 36 | 63.00% | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Slovakia** | 0 | 0 | - | 0 | 0 | - | 15 | 18 | 93.33% | 0 | 0 | - | 0 | 0 | - |
| **Slovenia** | 6 | 8 | 50.00% | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - | 0 | 0 | - |
| **Spain** | 479 | 715 | 51.00% | 647 | 954 | 55.00% | 927 | 1478 | 79.29% | 13 | 14 | 0.00% | 102 | 104 | 22.00% |
| **Sweden** | 54 | 66 | 54.00% | 36 | 71 | 33.00% | 281 | 825 | 87.54% | - | - | - | 7 | 7 | 4.00% |
| **United Kingdom** | 1975 | 2337 | 68.00% | 1274 | 1818 | 67.00% | 4404 | 6723 | 78.18% | 26 | 29 | 15.00% | 127 | 141 | 37.00% |
| **EU total** | **8589** | **10085** | **43.75%** | **8299** | **11039** | **44.83%** | **17738** | **30624** | **81.38%** | **97** | **119** | **22.00%** | **572** | **541** | **36.29%** |

## ANNEX 12: WHOIS DATABASE

The WHOIS is a directory service for domain names (such as "icann.org") allowing anyone to identify and contact the registered domain holder. This database is currently used by a wide variety of stakeholders for public safety purposes such as consumer protection, civil and criminal law enforcement, and cybersecurity incident mitigation. It is also used by individual consumers, for example to identify which party they are dealing with in a transaction, and by intellectual property right holders. The WHOIS information is collected and provided by a web of hundreds of registries and registrars. It includes over 60 data elements and policies, many of which potentially contain personal data.

A WHOIS record looks like this:



*Showing results for: ICANN.ORG*

Original Query: icann.org

### Contact Information

| Registrant Contact | Admin Contact | Tech Contact |
|---|---|---|
| Name: Domain Administrator | Name: Domain Administrator | Name: Domain Administrator |
| Organization: ICANN | Organization: ICANN | Organization: ICANN |
| Mailing Address: 12025 Waterfront Drive, Los Angeles California 90094-2536 US | Mailing Address: 12025 Waterfront Drive, Los Angeles California 90094-2536 US | Mailing Address: 12025 Waterfront Drive, Los Angeles California 90094-2536 US |
| Phone: +1.4242171313 | Phone: +1.4242171313 | Phone: +1.4242171313 |
| Ext: | Ext: | Ext: |
| Fax: +1.4242171313 | Fax: +1.4242171313 | Fax: +1.4242171313 |
| Fax Ext: | Fax Ext: | Fax Ext: |
| Email: domain-admin@icann.org | Email: domain-admin@icann.org | Email: domain-admin@icann.org |

### Registrar

WHOIS Server:
URL: http://www.godaddy.com
Registrar: GoDaddy.com, LLC
IANA ID: 146
Abuse Contact Email:
Abuse Contact Phone:

### Status

Domain Status: clientDeleteProhibited
https://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited
https://www.icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited
https://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited

The collection and publication of WHOIS information is required in the contracts which registries and registrars for so-called "generic" top-level domains (.com, .net etc) have with the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-profit membership-based corporation which coordinates the Domain Name System and a number of other vital Internet infrastructure elements.

The default option under the contracts is that all WHOIS data is publicly available. However, a number of gTLD registrars also provide "privacy and proxy[292]" services – usually at a charge – which allow for a domain name registrant to keep his or her identity private. According to recent statistics, this is the case for 15-20% of registrations. The privacy/proxy service provider can then provide information on the registrant upon individual request; policies for disclosing this information vary.

There is another set of top-level domains, the so-called "Country Code" top-level domains (ccTLDs), such as .de, .be or .uk. The ccTLD policies regarding registration, accreditation of registrars and WHOIS are managed according to the relevant oversight and governance mechanisms within the country, with no role for ICANN's Compliance department. ccTLDs use independent WHOIS lookup facilities[293]. In order to comply with local data protection rules, a number of ccTLD registries have implemented a "layered or gated" model, whereby they treat differently the registration of natural persons and that of companies or legal entities. For natural persons, certain personal data elements are not made publicly available: for instance, while the name of the registrant who is an natural person might be published, his telephone number, private address and email address are not visible to everyone and can only be accessed via specific channels, for instance through forms for individual requests. This has not created significant issues in the past, given that ccTLDs overall have much stricter registration policies and correspondingly much lower levels of abuse. The volume of requests therefore is not comparable to that generated by a gTLD registrar or registry with a less strict registration and anti-abuse policy.

To give an overall idea of the volumes involved, at the end of Q1 2017, there were 311 million domain names across all TLDs globally. ccTLDs have a combined market share of 40%, compared to 60% for gTLDs[294].

The public availability of WHOIS data has raised data protection concerns for a long time. With the approaching entry into application of the EU General Data Protection Regulation (GDPR) and its sanctions regime, the first registries and registrars, faced with uncertainty and fearing legal action, have stopped providing publicly available WHOIS information on the registrant when that registrant is not a corporate entity. Government representatives have voiced their concern over these developments, stating that "the continued and lawful availability of WHOIS/RDS data for consumer protection, intellectual property rights protection and law enforcement activities is a vital public concern and that ICANN should strive to explore all possible mechanisms under the GDPR to ensure that this data remains available for legitimate activities that protect the public and promote a safe, secure, and

[292] See here for more information.
[293] For an overview of European ones, see here.
[294] Council of European National Top-Level Domain Registries (CENTR), DomainWire – Global TLD Stat Report, Q1 2017.

trustworthy online environment."[295] For the EU, the Joint COM/EEAS Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' [296] also highlights this issue as a priority: "[…] online accountability should be further promoted. This means promoting measures to prevent the abuse of domain names for the distribution of unsolicited messages or phishing attacks. To this end, the Commission will work to improve the functioning of and the availability and accuracy of information in the Domain Name and IP WHOIS systems in line with the efforts of the Internet Corporation for Assigned Names and Numbers."

In the meantime, ICANN announced[297] on 2 November that it would temporarily suspend enforcement of the WHOIS policy, subject to a number of conditions. ICANN also published legal advice indicating that:

1. **WHOIS services will most likely need to change to** comply with data protection rules as the WHOIS database contains large quantities of personal data that is made available in an unfiltered manner to the general public. A legitimate interest for this service will be difficult to demonstrate.
2. Maintaining publicly available WHOIS can only be achieved through a series of complex policy changes and technical adjustments that are **unlikely** to be put in place. A possible solution would need to rely on consent of registrants which would need to be freely given and could be withdrawn at any moment. Registrants would need to be free to opt out.

The expert opinion also indicated that there was **lack of compliance with the existing rules**.

These announcements pave the way for a differentiated approach to the WHOIS. This could take the form of an expansion of privacy and proxy services or – in response to public interest concerns – a tiered access system, where a number of data elements would be available using credentialed access and for select groups of users only. This system has not been agreed upon, let alone implemented by all gTLD registries and registrars yet. However, it has been discussed for several years and at this point appears to be the only realistic option for the way forward, given that a full use of privacy and proxy services would have significant negative consequences for the public interest.

---

295 Governmental Advisory Committee (GAC), Consensus Advice to the ICANN Board of 1 November 2017, p11.

296 Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final.

297 See announcement here.

## ANNEX 13: SME TEST

### 1. Identification of affected businesses

SMEs are among the service providers affected by the measures described in this impact assessment, although it is estimated that up to 90% of current cross-border requests for non-content data are sent to five providers (Microsoft, Apple, google, Facebook, Twitter). This shows that SMEs account only for a small proportion of requests.

### 2. Consultation of SME stakeholders

SME stakeholders provided feedback to the Inception Impact Assessment and participated in the open public consultation through three industry associations: EuroIspa (one of the largest 'umbrella' associations of Internet Services Providers in the world, which includes a significant number of SMEs[298]), ACT | The App Association and ECO – German Internet Industry Association. All three raised concerns regarding the potential administrative burden and compliance costs, and two suggested that specific measures should be taken to reduce the financial cost. All however recognised the need for legal clarity.

In addition, the Commission had several meetings with EuroIspa, bilaterally and in the context of EU Internet Forum with several other service providers.

### 3. Measurement of the impact on SMEs

The different measures have been found to have the following impacts on SMEs:

***Baseline scenario***

The baseline scenario is characterised by a high degree of legal uncertainty. ACT (the app association) sums up the threat to SMEs in the face of legal uncertainty in their response to the Inception Impact Assessment: "While cloud computing has the potential to provide SME's with the ability to expand their business overseas at unprecedentedly low cost, legal uncertainty and retaliatory policies threaten this progress. Without a successful international framework to address cross-border law enforcement needs, nor one to address the digital economy, SME's face a legally and financially untenable situation in which they must discern which law governs in the context of extraterritorial warrants."[299]

[298] It represents over 2300 ISPs across the EU and EFTA countries - including ISPs from Austria, Belgium, the Czech Republic, Finland, France, Germany, Ireland, Italy, Norway, Romania and the UK. See here for more information .

[299] Accessible here.

***Non-legislative measures***

Given that the practical measures are largely voluntary in nature and do not require participation by all service providers, SMEs can participate where they deem measures cost-effective in view of their individual business model, corporate social responsibility and other factors. Therefore, the economic impact of the practical options does not go beyond the necessary and should not disfavour SMEs. On the contrary, SMEs should benefit disproportionately from higher-quality requests as might be ensured through a centralised SPOC system on the authorities' side. The possibility to opt into standardised forms and to draw upon streamlined policies for inspiration might furthermore have a positive economic impact, alleviating the cost burden for SMEs and contributing to ensure a level-playing field with bigger companies.

***International agreements***

In the absence of clarity as to the outcome of international negotiations, it is not possible to assess the impact of these measures on SMEs at this stage.

***Legislative measures***

Of the two legislative measures discussed, the European Production Order is the only which will have an impact on SMEs. The first important impact is that they would be faced by production orders from other Member States. This would affect both EU and non-EU SMEs. As also results from the replies to the public consultation, they would be faced with a relatively higher administrative burden than bigger companies, many of which already have staff and procedures in place to deal with foreign orders under voluntary cooperation. A particular burden would be to authenticate the orders to make sure they come from a legitimate source. This is much more difficult for a small company who only gets such order occasionally and is not familiar with the rules and procedures. On the other hand, as SMEs are particularly affected by legal uncertainty, they would benefit more from a clear legal framework in the EU and a unique procedure and form applied by all Member States. The fact that the form would be translated into their language would also make it easier for them.

Another important impact for SMEs will stem from the obligation to nominate a legal representative. This measure will mainly affect non-EU SMEs not present in the EU, as it will require nominating somebody in the EU. As noted by ACT – The App Association in its response to the Inception Impact Assessment, "[f]or small business service providers located outside of the EU, appointing a legal representative in the EU alone may represent an unsustainable cost, and could effectively prevent companies from doing business in the EU or with EU subjects."[300] On the other hand, this legal representative could be shared between service providers, in particular SMEs, and the legal representative may accumulate different functions (e.g. GDPR or ePrivacy representatives in addition to the production order legal

[300] Accessible here.

representative). It will only apply to SMEs who offer their services in the EU, and not in case of occasional data processing in the EU.

## 4. Assessment of alternative mechanisms and mitigating measures

The following mitigating measures were considered:

- Exempting SMEs from scope of measure on European Production Order

  After discussing this issue with Member States' experts, it has not been retained to exempt SMEs from the scope of the measure, as this would create a gap that could easily be exploited by criminals by moving to services offered by SMEs, and would seriously undermine the effectiveness of the measure.

- Exempting SMEs from scope of obligation to establish a legal representative

  For the same reason as above, it has not been retained to generally exempt SMEs from the scope of the obligation to nominate a legal representative. However, the obligation will not apply if data processing in the EU is only occasional, which could be the case for non-EU SMEs who have only a few customers in the EU.

- Cost reimbursement for all service providers

  A cost reimbursement system based on pre-defined rates exists in a few Member States for domestic procedures (e.g. AT, BE), but not in all. If such system is introduced EU-wide, it would have to apply to all service providers, not only to SMEs. Because 90% of all requests go to the big 5 service providers, such general cost reimbursement system would disproportionally affect Member States budgets, and would create an additional complexity to the system. Moreover, it is expected that those SMEs that would only be occasionally requested to produce data and that therefore would suffer the biggest administrative burden would also not be helped receiving a few Euro per request.

- Targeted guidance for SMEs

  To inform SMEs about the new legal framework and the obligations incumbent on them, the Commission would prepare guidance specifically addressed to them. This guidance could be disseminated with the help of industry associations.